

Dominion LX

Manuel d'utilisation
Version 2.4.5

LX-v2.4.5-0A-F

Octobre 2011

255-80-8009-00

Informations FCC (Etats-Unis seulement)

Cet équipement a été testé et certifié conforme aux limites d'un dispositif numérique de catégorie A selon l'article 15 du code de la Commission fédérale des communications des Etats-Unis (FCC). Ces limites visent à fournir une protection raisonnable contre les interférences nuisibles dans une installation commerciale. Cet équipement génère, utilise et peut émettre des émissions radioélectriques. S'il n'est pas installé et utilisé conformément aux instructions, il risque d'entraîner des interférences perturbant les communications radio. L'utilisation de l'équipement dans un environnement résidentiel peut générer des interférences nuisibles.

Informations VCCI (Japon)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan n'est pas responsable des dommages subis par ce produit suite à un accident, une catastrophe, une mauvaise utilisation, une modification du produit non effectuée par Raritan ou tout autre événement hors du contrôle raisonnable de Raritan ou ne découlant pas de conditions normales d'utilisation.



Consignes de sécurité pour montage en rack

Pour les produits Raritan qui doivent être montés en rack, prenez les précautions suivantes :

- La température de fonctionnement dans un environnement de rack fermé peut être supérieure à la température ambiante. Ne dépassez pas la température ambiante maximum recommandée des appareils. Reportez-vous à **Caractéristiques**.
- Assurez-vous que la circulation d'air dans l'environnement de rack est suffisante.
- Montez l'équipement dans le rack avec précaution de façon à éviter tout chargement bancal des composants mécaniques.
- Branchez l'équipement au circuit d'alimentation avec précaution afin d'éviter une surcharge des circuits.
- Mettez tout l'équipement correctement à la terre sur le circuit terminal, notamment les raccords d'alimentation tels que les barrettes d'alimentation (autres que celles branchées directement).

Table des matières

Annexe B Mise à jour du schéma LDAP 234

Annexe C Remarques d'informations 242

Chapitre 1 Introduction

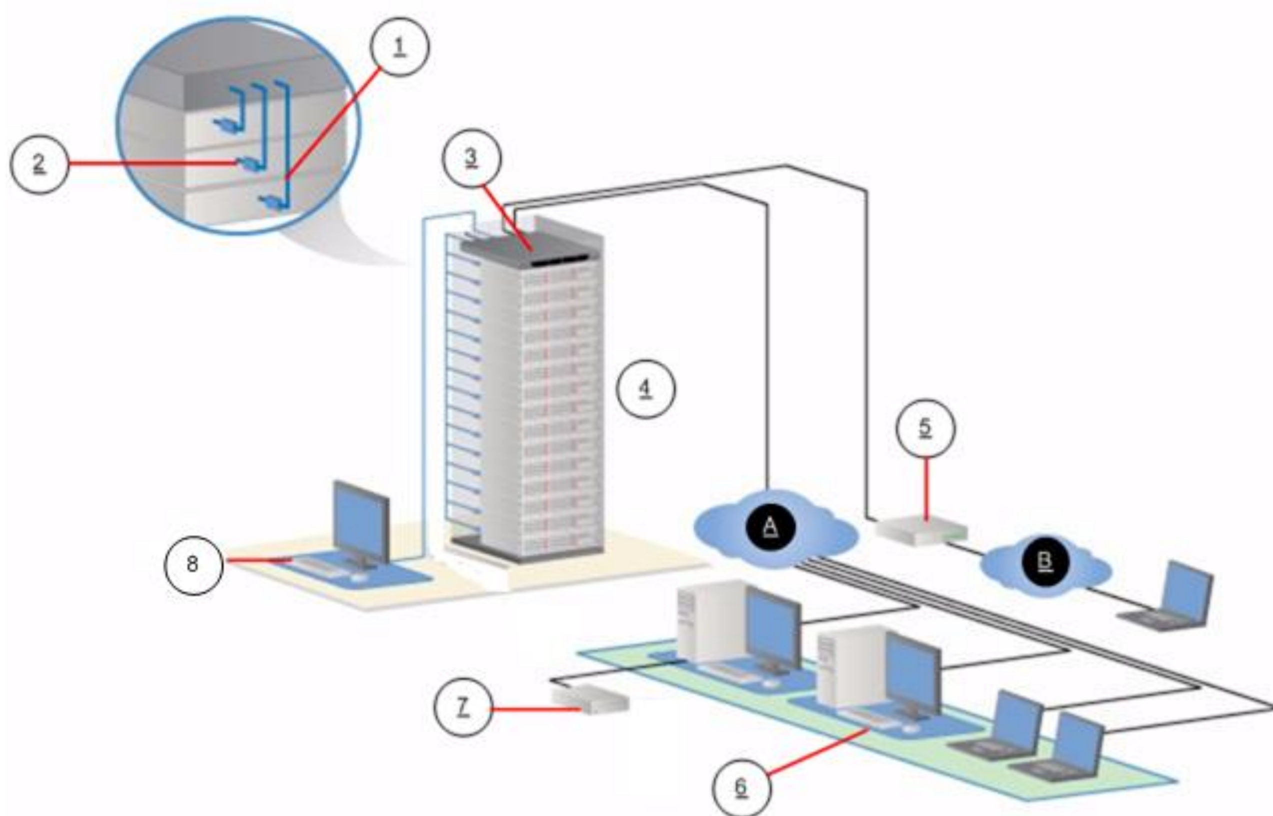
Dans ce chapitre

LX - Présentation

Les commutateurs KVM sur IP LX® donnent à un ou deux utilisateurs distants, disposant d'un port local indépendant, l'accès au niveau du BIOS à 16 serveurs au maximum et le contrôle de ces derniers. Lors de l'implémentation de la fonctionnalité multiniveau, les utilisateurs peuvent aisément contrôler jusqu'à 256 ordinateurs depuis une même console. Ces appareils, spécialement conçus pour les PME, offrent un accès à distance économique de n'importe où, une gestion des serveurs fiable et efficace, et un investissement initial minime offrant une évolutivité à moindre coût.

LX est fourni en standard avec la fonction Universal Virtual Media™ de Raritan, permettant le montage local d'une grande variété de lecteurs de CD, de DVD, USB, internes et distants, autorisant des tâches de gestion à distance et éliminant les déplacements. Vous disposez d'un affichage clair et net grâce à l'architecture moderne de la plate-forme, qui prend en charge une résolution vidéo distante haute définition (HD) 1920 x 1080 et une interface utilisateur par navigateur moderne et commune pour l'accès local et distant, nécessite une formation réduite, fournit une productivité sur le rack et assure une utilisation efficace de toutes les ressources informatiques. Les serveurs sont accessibles depuis Windows®, Linux®, Sun® ou Macintosh® via les navigateurs les plus répandus ou en mode autonome, sans frais de licence client.

Avec les options groupées de câblage, le personnel informatique des PME peut limiter l'investissement initial aujourd'hui tout en conservant la possibilité d'ajouter des fonctionnalités demain.



Légende			
1	Câble Cat5	6	Accès distant (réseau)
2	Module d'interface pour ordinateur (CIM)	7	Accès local
3	LX	A	Réseau IP local/étendu
4	Dispositifs KVM et série distants	B	RTPC
5	Modem		

Photos de LX



LX 108


Raritan
Dominion LX-116


RESET
LAN
MODEM

LX 116


Raritan
Dominion LX-216


RESET
LAN
MODEM

LX 216



Contenu de l'emballage

Chaque LX est un produit autonome entièrement configuré, dans un châssis de montage en rack 1U 19 pouces standard. Chaque dispositif LX est livré avec les éléments suivants :

Quantité	Elément
1	Dispositif LX
1	Kit de montage en rack
1	Cordon d'alimentation secteur
1	Manuel de configuration rapide LX
1	Note d'application
1	Carte de garantie

Applications clientes LX

Les applications clientes suivantes peuvent être utilisées dans LX :

Produit	Fonctionne avec...				
	MPC	RRC	VKC	RSC	AKC
LX 2.4.5 (ou supérieur)	✓		✓		✓

Reportez-vous au **manuel des clients KVM et série** pour en savoir plus sur les applications clientes. Reportez-vous également à la section ***Utilisation des serveurs cible*** (à la page 41) du présent manuel, qui contient des informations sur l'utilisation des clients avec LX.

Remarque : MPC et VKC requièrent Java™ Runtime Environment (JRE™). AKC est basé .NET.

Matériel

- Accès distant KVM sur IP intégré
- Modèles à 8 et 16 ports de serveurs
- Jusqu'à huit canaux vidéo permettant à deux utilisateurs au plus de se connecter à LX en même temps
- Fonction pour utilisateurs multiples (1/2 utilisateurs distants, 1 utilisateur local)
- Câblage de serveur UTP (Cat5/5e/6)
- Port Ethernet (10/100/1000 LAN)
- Améliorable en clientèle
- Port utilisateur local pour accès en rack
  - Trois ports USB 2.0 sur le panneau arrière pour les dispositifs USB pris en charge
  - Simultanéité complète avec l'accès utilisateur à distance
  - Interface graphique utilisateur (GUI) locale pour l'administration
- Prise en charge de modem
- Voyants à l'avant et à l'arrière indiquant le statut du dispositif, le démarrage et les mises à niveau de firmware
- Bouton de réinitialisation matérielle
- Port série pour la connexion à un modem externe.
- Montage en rack 19 pouces (supports de fixation fournis)

Logiciel

- Prise en charge des supports virtuels dans les environnements Windows®, Mac® et Linux® avec les CIM D2CIM-VUSB et D2CIM-DVUSB
- Balayage des ports et vue en miniature de cibles avec ensemble de balayage configurable
- Synchronisation absolue de la souris avec les CIM D2CIM-VUSB et D2CIM-DVUSB
- Plug and Play
- Gestion et accès Web
- Interface utilisateur graphique intuitive
- Chiffrement 256 bits de l'ensemble du signal KVM, signal vidéo et support virtuel inclus
- LDAP, Active Directory®, RADIUS ou authentification et autorisation internes
- Adressage DHCP ou IP fixe
- Gestion Syslog et SNMP
- Prise en charge d'IPv4 et d'IPv6
- LX et fonction multiniveau générique

Aide LX

L'aide LX explique comment installer, paramétrer et configurer LX. Elle comprend également des informations sur l'accès aux serveurs cible, à l'aide des supports virtuels, sur la gestion des utilisateurs et de la sécurité, ainsi que sur la maintenance et les diagnostics du produit LX.

Reportez-vous aux notes de version de LX pour obtenir des informations importantes sur la version en cours avant d'utiliser LX.

Une version PDF de l'aide peut être téléchargée de la page **Firmware and Documentation** du site Web de Raritan. Raritan vous recommande de consulter son site Web pour obtenir les derniers manuels d'utilisation disponibles.

Pour utiliser l'aide en ligne, Active Content (Contenu actif) doit être activé dans votre navigateur. Si vous utilisez Internet Explorer 7, vous devez activer Scriptlets. Consultez l'aide de votre navigateur pour en savoir plus sur l'activation de ces fonctions.

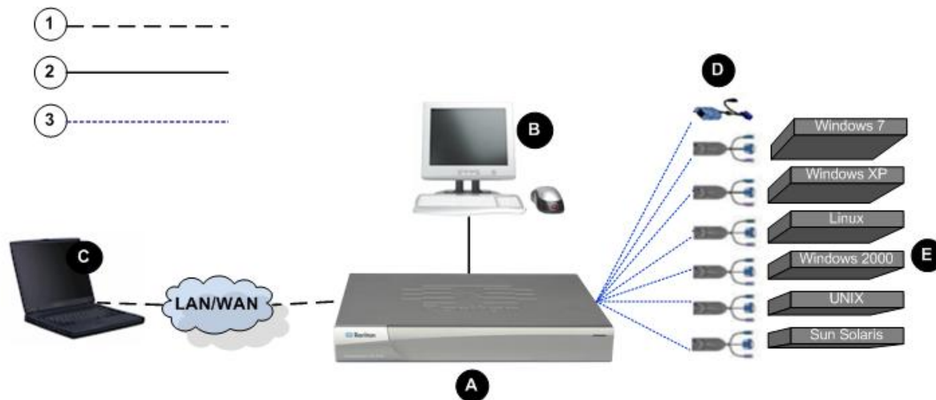
Documentation connexe

L'aide LX est accompagnée du manuel de configuration rapide LX, qui se trouve sur la page **Firmware and Documentation** du ***site Web de Raritan*** (***http://www.raritan.com/support/firmware-and-documentation***).

Les exigences et les instructions d'installation des applications clientes utilisées avec LX se trouvent dans le **manuel des clients d'accès KVM et série**, également présent sur le site Web de Raritan. Le cas échéant, des fonctions clientes particulières utilisées avec LX sont incluses dans l'aide.

Terminologie

L'aide utilise la terminologie suivante pour les composants LX types :



Légende du schéma	
1	TCP/IP IPv4 et/ou IPv6 ajoutés
2	KVM (clavier/vidéo/souris)
3	Câble UTP (Cat5/5e/6)
A	LX
B	Console d'accès local (Local Access Console) Utilisateur local - Console utilisateur facultative (constituée d'un clavier, d'une souris et d'un écran VGA Multisync) directement reliée à LX pour gérer des serveurs cible KVM (directement au niveau du rack et non par l'intermédiaire du réseau).
C	Ordinateur distant (Remote PC) Ordinateurs mis en réseau utilisés pour accéder aux serveurs cible connectés à LX et les gérer.
D	CIM Clés qui se connectent sur chaque serveur cible. Disponibles pour tous les systèmes d'exploitation pris en charge.
E	Serveurs cible (Target Servers) Serveurs cible KVM - Serveurs disposant de cartes vidéo et d'interfaces utilisateur (par exemple, système d'exploitation Windows®, Linux®, Solaris™, etc.) et accessibles à distance via LX.

Reportez-vous à CIM et systèmes d'exploitation pris en charge - LX pour obtenir la liste des systèmes d'exploitation et des CIM pris en charge.

Chapitre 2 Installation et configuration

Dans ce chapitre

Présentation

Cette section propose un bref aperçu du processus d'installation. Chaque étape est décrite en détails dans les autres sections de ce chapitre.

Pour installer et configurer LX :

- ***Etape 1 : Configuration des serveurs cible KVM*** (à la page 13)
- ***Etape 2 : Configuration des paramètres du pare-feu de réseau*** (à la page 29)
- ***Etape 3 : Connexion de l'équipement*** (à la page 29)
- ***Etape 4 : Configuration de LX*** (à la page 32)
- ***Etape 5 : Lancement de la console distante de LX*** (à la page 37)
- ***Etape 6 : Configuration de la langue du clavier (facultatif)*** (à la page 38)
- ***Etape 7 : Configuration de la fonction multiniveau (facultatif)*** (à la page 39)

Vous trouverez également dans cette section les données de connexion par défaut dont vous aurez besoin. Particulièrement, l'adresse IP, le nom d'utilisateur et le mot de passe par défaut. Reportez-vous à ***Données de connexion par défaut*** (à la page 12).

Données de connexion par défaut

Valeur par défaut	Valeur
Nom d'utilisateur	Le nom d'utilisateur par défaut est admin. Cet utilisateur dispose de droits d'administrateur.
Mot de passe	Le mot de passe par défaut est raritan. Les mots de passe respectent la casse, doivent être saisis exactement de la même manière que lors de leur création. Par exemple, le mot de passe par défaut raritan doit être saisi uniquement en lettres minuscules.

Valeur par défaut	Valeur
	La première fois que vous démarrez LX, il vous est demandé de changer le mot de passe par défaut.
IP address (Adresse IP)	LX est fourni avec l'adresse IP par défaut 192.168.0.192.

Important : à des fins de sauvegarde et de continuité des opérations, il est fortement recommandé de créer un nom d'utilisateur et un mot de passe de secours pour l'administrateur, et de conserver ces données dans un endroit sûr.

Mise en route

Etape 1 : Configuration des serveurs cible KVM

Les serveurs cible KVM sont des ordinateurs accessibles et contrôlés via LX. Avant d'installer LX, configurez tous les serveurs cible KVM afin d'obtenir des performances optimales. Cette configuration s'applique aux serveurs cible KVM uniquement, non aux postes de travail clients (ordinateurs distants) utilisés pour accéder à distance à LX.

Papier peint du Bureau

Pour une utilisation de bande passante et une qualité vidéo optimales, utilisez dans la mesure du possible des couleurs de fond unies. Les fonds comportant des photos ou des gradients complexes risquent de nuire aux performances.

Résolutions vidéo prises en charge

Assurez-vous que la résolution vidéo et le taux de rafraîchissement de chaque serveur cible sont pris en charge par l'unité LX, et que le signal est non entrelacé.

La résolution vidéo et la longueur de câble sont des facteurs importants dans la réalisation de la synchronisation de la souris. Reportez-vous à ***Distance de connexion et résolution vidéo du serveur cible*** (à la page 226).

L'unité LX prend en charge ces résolutions :

Résolutions	
640 x 350 à 70Hz	1024 x768 à 85
640 x 350 à 85Hz	1024 x 768 à 75Hz
640 x 400 à 56Hz	1024 x 768 à 90Hz
640 x 400 à 84Hz	1024 x 768 à 100Hz
640 x 400 à 85Hz	1152 x 864 à 60Hz
640 x 480 à 60Hz	1152 x 864 à 70Hz
640 x 480 à 66,6Hz	1152 x 864 à 75Hz
640 x 480 à 72Hz	1152 x 864 à 85Hz
640 x 480 à 75Hz	1152 x 870 à 75,1Hz
640 x 480 à 85Hz	1152 x 900 à 66Hz
720 x 400 à 70Hz	1152 x 900 à 76Hz
720 x 400 à 84Hz	1280 x 720 à 60Hz
720 x 400 à 85Hz	1280 x 960 à 60Hz
800 x 600 à 56Hz	1280 x 960 à 85Hz
800 x 600 à 60Hz	1280 x 1024 à 60Hz
800 x 600 à 70Hz	1280 x 1024 à 75Hz
800 x 600 à 72Hz	1280 x 1024 à 85Hz
800 x 600 à 75Hz	1360 x 768 à 60Hz
800 x 600 à 85Hz	1366 x 768 à 60Hz
800 x 600 à 90Hz	1368 x 768 à 60Hz
800 x 600 à 100Hz	1400 x 1050 à 60Hz
832 x 624 à 75,1Hz	1440 x 900 à 60Hz

Résolutions	
1024 x 768 à 60Hz	1600 x 1200 à 60Hz
1024 x 768 à 70	1680 x 1050 à 60Hz
1024 x 768 à 72	1920 x 1080 à 60Hz

Modes souris

LX fonctionne en modes Absolute Mouse Mode™ (mode souris absolue), Intelligent Mouse Mode (mode souris intelligente) et Standard Mouse Mode (mode souris standard).

Les paramètres de souris n'ont pas besoin d'être modifiés pour la synchronisation absolue de la souris mais un module D2CIM-VUSB ou D2CIM-DVUSB est requis. Quel que soit le mode souris suivant : standard ou intelligente, les paramètres de la souris doivent être configurés sur des valeurs spécifiques. Les configurations de souris varient selon les différents systèmes d'exploitation cible. Reportez-vous à la documentation de votre système d'exploitation pour de plus amples informations.

Le mode souris intelligente fonctionne bien sur la plupart des plates-formes Windows, mais peut produire des résultats imprévisibles lorsque Active Desktop est défini sur la cible. N'utilisez pas de souris animée pour le mode souris intelligente.

Paramètres Windows XP, Windows 2003 et Windows 2008

► **Pour configurer les serveurs cible KVM exécutant le système d'exploitation Microsoft® Windows XP®, le système d'exploitation Windows 2003® ou les systèmes d'exploitation Windows 2008® :**

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Panneau de configuration > Souris.
   b. Cliquez sur l'onglet Options du pointeur.
   c. Dans la partie Mouvement du pointeur :

- Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
- Désactivez l'option Améliorer la précision du pointeur.
- Désactivez l'option Alignement.
- Cliquez sur OK.

Remarque : lorsque vous exécutez Windows 2003 sur votre serveur cible et que vous accédez au serveur via KVM et effectuez l'une des actions répertoriées ci-dessous, la synchronisation de la souris peut être perdue si elle était déjà activée. Il vous faudra sélectionner la commande Synchronize Mouse (Synchroniser la souris) dans le menu Mouse (Souris) du client pour la réactiver. Les actions ci-après peuvent provoquer ce problème :

- Ouvrir un éditeur de texte.

- Accéder aux propriétés de la souris, du clavier et options de modem et de téléphonie à partir du Panneau de configuration Windows.

---

2. Désactivez les effets de transition :
   a. Sélectionnez l'option Affichage du Panneau de configuration.
   b. Cliquez sur l'onglet Apparence.
   c. Cliquez sur Effets.
   d. Désélectionnez la case Utiliser l'effet de transition suivant pour les menus et les info-bulles.
   e. Cliquez sur OK.
3. Fermez le Panneau de configuration.

Remarque : pour les serveurs cible KVM exécutant Windows XP, Windows 2000 ou Windows 2008, vous pouvez créer un nom d'utilisateur qui servira uniquement pour les connexions à distance via LX. Vous pourrez ainsi réserver aux connexions LX les paramètres d'accélération/de mouvement lent du pointeur de la souris définis pour le serveur cible.

Les pages de connexion de Windows XP, 2000 et 2008 rétablissent les paramètres prédéfinis de la souris qui diffèrent de ceux suggérés pour des performances optimales de l'unité LX. En conséquence, il est possible que la synchronisation de la souris ne soit pas optimale pour ces écrans.

Remarque : Effectuez cette opération uniquement si vous êtes capable de manipuler le Registre des serveurs cible KVM Windows. Vous pouvez obtenir une meilleure synchronisation de la souris LX aux pages de connexion en utilisant l'éditeur du Registre Windows pour modifier les paramètres suivants : HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Paramètres Windows 7 et Windows Vista

Pour configurer les serveurs cible KVM exécutant le système d'exploitation Windows Vista® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Paramètres > Panneau de configuration > Souris.
   b. Sélectionnez Paramètres système avancés dans le panneau de navigation à gauche. La boîte de dialogue Propriétés système s'affiche.
   c. Cliquez sur l'onglet Options du pointeur.
   d. Dans la partie Mouvement du pointeur :
      - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
      - Désactivez l'option Améliorer la précision du pointeur.
      - Cliquez sur OK.
2. Désactivez les effets de fondu et d'animation :
   a. Sélectionnez l'option Système à partir du Panneau de configuration.
   b. Sélectionnez Informations sur les performances et Outils > Outils avancés > Ajuster pour régler l'apparence et les performances de Windows.
   c. Cliquez sur l'onglet Avancé.
   d. Cliquez sur Paramètres dans le groupe Performances pour ouvrir la boîte de dialogue Options de performances.

e. Sous les options Personnalisation, désélectionnez les cases à cocher suivantes :

- Options d'animation :
  - Animer les commandes et les éléments à l'intérieur des fenêtres
  - Animer les fenêtres lors de la réduction et de l'agrandissement
- Options de fondu :
  - Fondre ou faire glisser les menus dans la zone de visualisation
  - Fondre ou faire glisser les info-bulles dans la zone de visualisation
  - Fermer en fondu les commandes de menu après le clic de souris

3. Cliquez sur OK et fermez le Panneau de configuration.

Pour configurer les serveurs cible KVM exécutant le système d'exploitation Windows 7® :

1. Définissez les paramètres de la souris :

a. Sélectionnez Démarrer > Panneau de configuration > Matériel et audio > Souris.

b. Cliquez sur l'onglet Options du pointeur.

c. Dans la partie Mouvement du pointeur :

- Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
- Désactivez l'option Améliorer la précision du pointeur.
- Cliquez sur OK.

2. Désactivez les effets de fondu et d'animation :

a. Sélectionnez Panneau de configuration > Système et sécurité.

b. Sélectionnez Système, puis Paramètres système avancés dans le panneau de navigation à gauche. La fenêtre Propriétés système s'affiche.

c. Cliquez sur l'onglet Avancé.

d. Cliquez sur le bouton Paramètres du groupe Performances pour ouvrir la boîte de dialogue Options de performances.

e. Sous les options Personnalisation, désélectionnez les cases à cocher suivantes :

- Options d'animation :

        - Animer les commandes et les éléments à l'intérieur des fenêtres
        - Animer les fenêtres lors de la réduction et de l'agrandissement
    - Options de fondu :
        - Fondre ou faire glisser les menus dans la zone de visualisation
        - Fondre ou faire glisser les info-bulles dans la zone de visualisation
        - Fermer en fondu les commandes de menu après le clic de souris
3. Cliquez sur OK et fermez le Panneau de configuration.

Paramètres Windows 2000

Pour configurer les serveurs cible KVM exécutant le système d'exploitation Microsoft Windows® 2000® :

1. Définissez les paramètres de la souris :
    a. Sélectionnez Démarrer > Panneau de configuration > Souris.
    b. Cliquez sur l'onglet Motion (Mouvement).
        - Définissez l'accélération du pointeur sur Aucune.
        - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
        - Cliquez sur OK.
2. Désactivez les effets de transition :
    a. Sélectionnez l'option Affichage du Panneau de configuration.
    b. Cliquez sur l'onglet Effets.
        - Désélectionnez la case Utiliser l'effet de transition suivant pour les menus et les info-bulles.
3. Cliquez sur OK et fermez le Panneau de configuration.

Remarque : pour les serveurs cible KVM exécutant Windows XP, Windows 2000 ou Windows 2008, vous pouvez créer un nom d'utilisateur qui servira uniquement pour les connexions à distance via LX. Vous pourrez ainsi réserver aux connexions LX les paramètres d'accélération/de mouvement lent du pointeur de la souris définis pour le serveur cible.

Les pages de connexion de Windows XP, 2000 et 2008 rétablissent les paramètres prédéfinis de la souris qui diffèrent de ceux suggérés pour des performances optimales de l'unité LX. En conséquence, il est possible que la synchronisation de la souris ne soit pas optimale pour ces écrans.

Remarque : Effectuez cette opération uniquement si vous êtes capable de manipuler le Registre des serveurs cible KVM Windows. Vous pouvez obtenir une meilleure synchronisation de la souris LX aux pages de connexion en utilisant l'éditeur du Registre Windows pour modifier les paramètres suivants : HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Paramètres Linux (Red Hat 9)

Remarque : les paramètres suivants sont optimisés uniquement pour le mode souris standard.

▶ Pour configurer les serveurs cible KVM exécutant Linux® (interface utilisateur graphique) :

1. Définissez les paramètres de la souris :
   a. Choisissez Main Menu > Preferences > Mouse (Menu principal > Préférences > Souris). La boîte de dialogue des préférences de la souris s'affiche.
   b. Cliquez sur l'onglet Motion (Mouvement).
   c. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
   d. Dans la même section, définissez également une faible sensibilité.
   e. Dans la section du glisser-déposer, définissez un seuil faible.
   f. Fermez la boîte de dialogue des préférences de la souris.

   Remarque : si ces étapes ne fonctionnent pas, saisissez la commande xset mouse 1 1, comme décrit dans les instructions de ligne de commande Linux.

   ---

2. Définissez la résolution d'écran :
   a. Choisissez Main Menu > System Settings > Display (Menu principal > Paramètres système > Affichage). La boîte de dialogue des paramètres d'affichage apparaît.

b. Dans l'onglet Display (Affichage), sélectionnez une résolution prise en charge par LX.

c. Dans l'onglet Advanced (Avancé), vérifiez que le taux de rafraîchissement est pris en charge par LX.

Remarque : dans la plupart des environnement graphiques Linux, une fois que la connexion au serveur cible est établie, la commande <Ctrl> <Alt> <+> change la résolution vidéo en faisant défiler toutes les résolutions disponibles activées dans le fichier XF86Config ou /etc/X11/xorg.conf, suivant la distribution de votre serveur X.

▸ Pour configurer les serveurs cible KVM exécutant Linux (ligne de commande) :

1. Définissez l'accélération du pointeur de la souris et le seuil exactement sur 1. Entrez la commande suivante : *xset mouse 1 1*. Ce paramètre doit est réglé pour être exécuté lorsque vous vous connectez.
2. Assurez-vous que tous les serveurs cible exécutant Linux utilisent une résolution VESA standard et un taux de rafraîchissement pris en charge par LX.
3. Les serveurs cible Linux doivent également être configurés de manière à ce que les temps de passage en blanc correspondent aux valeurs VESA standard +/- 40 % :

   a. Localisez le fichier de configuration Xfree86 (XF86Config).

   b. Désactivez toutes les résolutions qui ne sont pas prises en charge par LX à l'aide d'un éditeur de texte.

   c. Désactivez la fonctionnalité de bureau virtuel (non prise en charge par LX).

   d. Vérifiez les temps de passage en blanc (valeurs VESA standard +/- 40 %).

   e. Redémarrez l'ordinateur.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Remarque concernant les serveurs cible KVM Red Hat 9

Si vous exécutez Red Hat® 9 sur le serveur cible à l'aide d'un CIM USB, et que vous rencontrez des problèmes avec le clavier et/ou la souris, vous pouvez essayer un autre paramètre de configuration.

Conseil : ces étapes peuvent se révéler nécessaires même après une installation propre du SE.

Pour configurer les serveurs Red Hat 9 à l'aide de CIM USB :

1. Recherchez le fichier de configuration (généralement /etc/modules.conf) sur le système.
2. Ouvrez l'éditeur de votre choix et assurez-vous que la ligne alias usb-controller du fichier modules.conf est comme suit :

   alias usb-controller usb-uhci

   Remarque : si une autre ligne fait apparaître usb-uhci dans le fichier /etc/modules.conf, elle doit être supprimée ou mise en commentaire.

3. Enregistrez le fichier.
4. Redémarrez le système pour que les modifications soient appliquées.

Paramètres Linux (Red Hat 4)

Remarque : les paramètres suivants sont optimisés uniquement pour le mode souris standard.

Pour configurer les serveurs cible KVM exécutant Linux® (interface utilisateur graphique) :

1. Définissez les paramètres de la souris :
   a. Pour les utilisateurs de Red Hat 5 : Choisissez Main Menu > Preferences > Mouse (Menu principal > Préférences > Souris). Pour les utilisateurs de Red Hat 4 : Choisissez Main Menu > Preferences > Mouse (Menu principal > Préférences > Souris). La boîte de dialogue des préférences de la souris s'affiche.
   b. Cliquez sur l'onglet Mouvement.
   c. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
   d. Dans la même section, définissez également une faible sensibilité.
   e. Dans la section du glisser-déposer, définissez un seuil faible.

f. Fermez la boîte de dialogue des préférences de la souris.

Remarque : si ces étapes ne fonctionnent pas, saisissez la commande xset mouse 1 1, comme décrit dans les instructions de ligne de commande Linux.

---

2. Définissez la résolution d'écran :
   a. Choisissez Main Menu > System Settings > Display (Menu principal > Paramètres système > Affichage). La boîte de dialogue des paramètres d'affichage apparaît.
   b. Dans l'onglet Settings (Paramètres), sélectionnez une résolution prise en charge par LX.
   c. Cliquez sur OK.

Remarque : dans la plupart des environnement graphiques Linux, une fois que la connexion au serveur cible est établie, la commande <Ctrl> <Alt> <+> change la résolution vidéo en faisant défiler toutes les résolutions disponibles activées dans le fichier XF86Config ou /etc/X11/xorg.conf, suivant la distribution de votre serveur X.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Paramètres SUSE Linux 10.1

Remarque : n'essayez pas de synchroniser la souris à l'invite de connexion SUSE Linux®. Vous devez être connecté au serveur cible pour synchroniser les curseurs de souris.

▶ Pour configurer les paramètres de la souris :

1. Choisissez Desktop > Control Center (Bureau > Centre de contrôle). La boîte de dialogue des préférences du bureau s'affiche.
2. Cliquez sur Mouse (Souris). La boîte de dialogue des préférences de la souris s'affiche.
3. Ouvrez l'onglet Motion (Mouvement).
4. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
5. Dans la même section, définissez également une faible sensibilité.
6. Dans la section du glisser-déposer, définissez un seuil faible.
7. Cliquez sur Fermer.

▶ Pour configurer la vidéo :

1. Choisissez Desktop Preferences > Graphics Card and Monitor (Préférences du bureau > Carte graphique et moniteur). La boîte de dialogue des propriétés de la carte et du moniteur s'affiche.

2. Vérifiez que la résolution et le taux de rafraîchissement utilisés sont pris en charge par LX. Reportez-vous à **Résolutions vidéo prises en charge** pour plus d'informations.

   Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Rendre les paramètres Linux permanents

Remarque : ces étapes peuvent varier légèrement selon la version de Linux® utilisée.

▶ Pour rendre vos paramètres dans Linux permanents (invite) :

1. Choisissez System Menu > Preferences > Personal > Sessions (Menu système > Préférences > Personnel > Sessions).
2. Cliquez sur l'onglet Session Options (Options de session).
3. Activez l'option Prompt on log off (Invite à la déconnexion), puis cliquez sur OK. Cette option vous invite à enregistrer la session en cours lorsque vous vous déconnectez.
4. Au moment de la déconnexion, activez l'option Save current setup (Enregistrer la configuration actuelle) dans la boîte de dialogue.
5. Cliquez sur OK.

Conseil : pour empêcher que cette invite ne s'affiche lorsque vous vous déconnectez, exécutez la procédure suivante.

▶ Pour rendre vos paramètres dans Linux permanents (sans invite) :

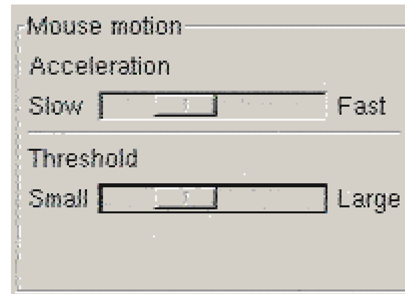
1. Choisissez Desktop (Bureau) > Control Center (Centre de contrôle) > System (Système) > Sessions.
2. Cliquez sur l'onglet Session Options (Options de session).
3. Désactivez la case à cocher Prompt on the log off (Invite à la déconnexion).
4. Activez l'option Automatically save changes to the session (Enregistrer automatiquement les modifications de la session), puis cliquez sur OK. Cette option enregistre automatiquement votre session actuelle au moment de la déconnexion.

Paramètres Sun Solaris

▶ Pour configurer les serveurs cible KVM exécutant Sun™ Solaris™ :

1. Définissez la valeur d'accélération du pointeur de la souris et le seuil exactement sur 1. Cela peut être effectué :

- à partir de l'interface utilisateur graphique ;



- à partir de la ligne de commande *xset mouse a t* où *a* représente l'accélération et *t*, le seuil.

2. Tous les serveurs cible KVM doivent être configurés en utilisant l'une des résolutions d'affichage prises en charge par LX. Les résolutions les plus courantes sur les ordinateurs Sun sont :

Résolution d'affichage	Taux de rafraîchissement vertical	Rapport hauteur/largeur
1600 x 1200	60 Hz	4:3
1280 x 1024	60, 75, 85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60, 70, 75, 85 Hz	4:3
800 x 600	56, 60, 72, 75, 85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60, 72, 75, 85 Hz	4:3

3. Les serveurs cible KVM exécutant le système d'exploitation Solaris doivent utiliser une sortie vidéo VGA (signaux H-Sync et V-Sync, pas à synchronisation composite).

Pour passer d'une sortie de carte graphique Sun synchronisée de manière composite à une sortie VGA non standard :

1. Lancez la commande Stop+A pour afficher le mode bootprom.
2. Lancez la commande suivante pour modifier la résolution de sortie : *setenv output-device screen:r1024x768x70*
3. Lancez la commande `boot` pour redémarrer le serveur.

Vous pouvez également vous procurer un adaptateur de sortie vidéo auprès de votre revendeur Raritan.

Si vous avez	Utilisez cet adaptateur de sortie vidéo
Sun 13W3 avec une sortie synchronisée de manière composite	convertisseur APSSUN II Guardian.
Sun HD15 avec une sortie synchronisée de manière composite	convertisseur 1396C pour convertir de HD15 à 13W3 et un convertisseur APSSUN II Guardian pour prendre en charge la synchronisation composite.
Sun HD15 avec une sortie synchronisée de manière séparée	convertisseur APKMSUN Guardian.

Remarque : certains écrans d'arrière-plan Sun ne se centrent pas toujours précisément sur les serveurs Sun ayant des bordures sombres. Utilisez un autre arrière-plan ou une icône de couleur claire dans le coin supérieur gauche.

Paramètres de souris

Pour configurer les paramètres de la souris (Sun Solaris 10.1) :

1. Choisissez Launcher (Lancement). Application Manager - Desktop Controls (Gestionnaire d'applications - Contrôles de bureau) apparaît.
2. Sélectionnez Mouse Style Manager (Gestionnaire du style de souris). La boîte de dialogue Style Manager - Mouse (Gestionnaire de style - Souris) apparaît.
3. Définissez Acceleration sur 1.0.
4. Définissez Threshold (Seuil) sur 1.0.
5. Cliquez sur OK.

Accès à la ligne de commande

1. Cliquez avec le bouton droit de la souris.
2. Sélectionnez Tools (Outils) > Terminal. Une fenêtre de terminal s'ouvre. (Il est préférable de se trouver à la racine pour lancer des commandes.)

Paramètres vidéo (POST)

Les systèmes Sun ont deux paramètres de résolution différents : une résolution POST et une résolution GUI. Exécutez ces commandes depuis la ligne de commande.

Remarque : les valeurs 1024x768x75 sont utilisées ici à titre d'exemple. Remplacez ces paramètres par la résolution et le taux de rafraîchissement que vous utilisez.

Pour vérifier la résolution POST actuelle :

- Exécutez la commande suivante à la racine : `# eeprom output-device`

Pour modifier la résolution POST :

1. Exécutez `# eeprom output-device=screen:r1024x768x75`.
2. Déconnectez-vous ou redémarrez l'ordinateur.

Paramètres vidéo (GUI)

La résolution GUI peut être vérifiée et définie à l'aide de différentes commandes selon la carte vidéo utilisée. Exécutez ces commandes depuis la ligne de commande.

Remarque : les valeurs 1024x768x75 sont utilisées ici à titre d'exemple. Remplacez ces paramètres par la résolution et le taux de rafraîchissement que vous utilisez.

Carte	Pour vérifier la résolution :	Pour modifier la résolution :
32 bits	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.
64 bits	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.
32 bits et 64 bits	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.

Paramètres IBM AIX 5.3

Suivez la procédure ci-après pour configurer les serveurs cible KVM exécutant IBM® AIX™ 5.3.

Pour configurer la souris :

1. Démarrez le lanceur.
2. Sélectionnez Style Manager (Gestionnaire de style).
3. Cliquez sur Mouse (Souris). La boîte de dialogue Style Manager - Mouse (Gestionnaire de style - Souris) apparaît.
4. Définissez Mouse acceleration (Accélération de la souris) sur 1.0 et Threshold (Seuil) sur 1.0.
5. Cliquez sur OK.

Pour configurer la vidéo :

1. Depuis le lanceur, sélectionnez Application Manager (Gestionnaire d'applications).
2. Sélectionnez System_Admin.
3. Sélectionnez Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate (Smit > Dispositifs > Affichages graphiques > Sélectionner la résolution d'affichage et le taux de rafraîchissement).
4. Sélectionnez la carte vidéo utilisée.
5. Cliquez sur List. Une liste de modes d'affichage apparaît.
6. Sélectionnez une résolution et un taux de rafraîchissement pris en charge par LX. Reportez-vous à Résolutions vidéo prises en charge pour plus d'informations.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Rendre les paramètres UNIX permanents

Remarque : ces étapes peuvent varier légèrement selon le type d'UNIX® (par exemple, Solaris™, IBM® AIX™) et la version utilisée.

---

1. Sélectionnez Style Manager (Gestionnaire de style) > Startup (Démarrage). La boîte de dialogue Style Manager - Startup (Gestionnaire de style - Démarrage) apparaît.
2. Dans la fenêtre Logout Confirmation (Confirmation de connexion), sélectionnez l'option On (Activé). Cette option vous invite à enregistrer la session en cours lorsque vous vous déconnectez.

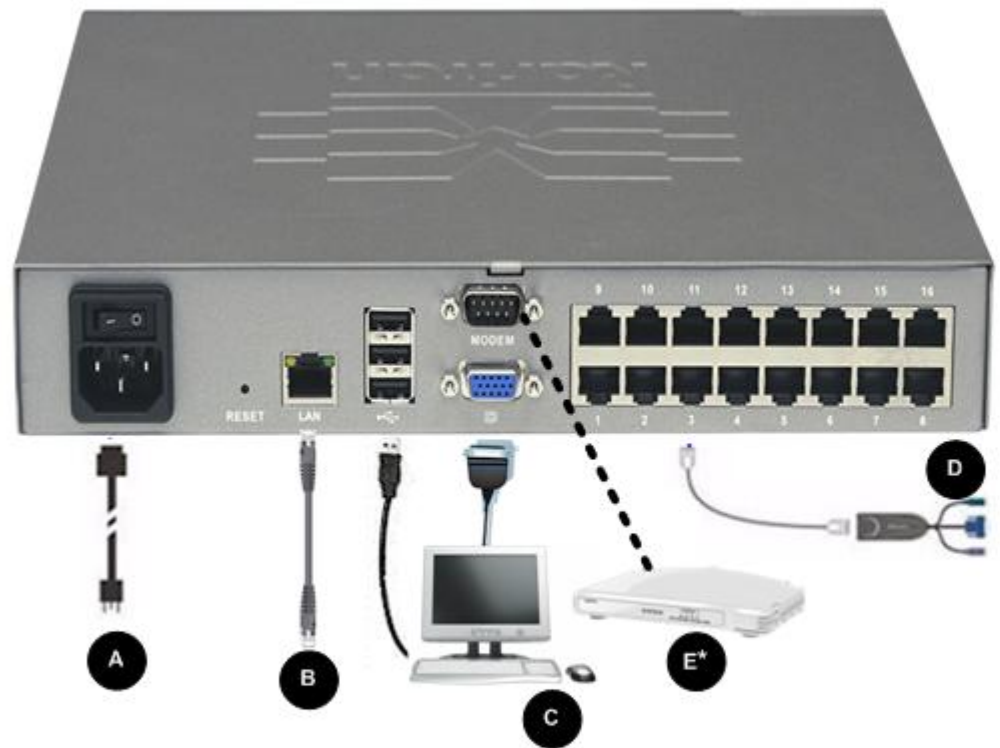
Paramètres Apple Macintosh

Sur les serveurs cible KVM exécutant le système d'exploitation Apple Macintosh®, la meilleure solution est d'utiliser la technologie D2CIM-VUSB et la synchronisation absolue de la souris.

Etape 2 : Configuration des paramètres du pare-feu de réseau

Pour permettre l'accès distant à LX, vos réseau et pare-feu doivent autoriser la communication sur le port TCP 5000. Vous pouvez également configurer l'unité LX pour utiliser un autre port TCP, puis autoriser la communication sur ce port. Pour accéder à LX par le biais d'un navigateur Web, votre pare-feu doit autoriser l'accès au port TCP 443 (port standard HTTPS). L'accès au port TCP 80 (port standard HTTP) permet de rediriger automatiquement les requêtes HTTP vers HTTPS.

Etape 3 : Connexion de l'équipement



A. Alimentation CA

Pour connecter l'alimentation :

- Raccordez le cordon d'alimentation CA fourni avec LX et branchez-le sur une prise électrique.

B. Port réseau

Pour connecter le réseau :

- Reliez un câble Ethernet standard (fourni) du port réseau à un commutateur, concentrateur ou routeur Ethernet.

C. Port pour accès local (PC local)

Pour accéder facilement aux serveurs cible sur le rack, utilisez le port d'accès local de LX. Si le port d'accès local est obligatoire pour l'installation et le paramétrage, il est facultatif par la suite. Le port d'accès local fournit également une interface utilisateur graphique depuis la console locale de LX pour l'administration et l'accès au serveur cible. Reportez-vous à Configuration des paramètres du port local de LX pour plus d'informations.

Pour connecter le port local :

- Reliez un écran VGA Multisync, une souris et un clavier aux ports Local User (Utilisateur local) respectifs ; utilisez un clavier et une souris USB. Les connexions de port sont situées sur le panneau arrière de LX.

Connexion	Description
Ecran	Branchez un écran VGA Multisync standard sur le port vidéo HD15 (femelle).
Clavier	Branchez un clavier USB standard à un des ports USB de type A (femelle).
Souris	Branchez une souris USB standard à un des ports USB de type A (femelle).

D. Ports de serveur cible

Pour accéder facilement aux serveurs cible sur le rack, utilisez le port d'accès local de LX. Si le port d'accès local est obligatoire pour l'installation et le paramétrage, il est facultatif par la suite. Le port d'accès local fournit également une interface utilisateur graphique depuis la console locale de LX pour l'administration et l'accès au serveur cible. Reportez-vous à Configuration des paramètres du port local de LX pour plus d'informations.

Pour connecter un serveur cible à LX :

1. Utilisez le module CIM (Computer Interface Module) approprié. Reportez-vous à ***Systèmes d'exploitation pris en charge (clients)*** (à la page 222) pour plus d'informations sur les CIM compatibles.
2. Connectez le câble UTP (Cat5/5e/6) de votre CIM au port vidéo de votre serveur cible. Vérifiez que la vidéo du serveur cible est déjà configurée sur une résolution et un taux de rafraîchissement pris en charge. Pour les serveurs Sun, assurez-vous que la carte vidéo du serveur cible est définie sur une sortie VGA standard (Sync H-et-V) et non Sync Composite.
3. Reliez le connecteur clavier/souris de votre CIM aux ports correspondants du serveur cible. A l'aide d'un câble UTP à brochage direct standard (Cat5/5e/6), raccordez le CIM à un port serveur disponible à l'arrière du dispositif LX.

Remarque : DCIM-USB G2 présente un petit commutateur à l'arrière du CIM. Placez ce commutateur sur P pour les serveurs cible USB PC. Placez ce commutateur sur S pour les serveurs cible USB Sun.

Une nouvelle position de commutateur ne prend effet qu'après l'alimentation cyclique du CIM. Pour effectuer l'alimentation cyclique du CIM, retirez le connecteur USB du serveur cible, puis rebranchez-le quelques secondes plus tard.

E. Port du modem (facultatif)

LX dispose d'un port modem dédié qui permet l'accès à distance même lorsque le réseau local/réseau étendu n'est pas disponible. Utilisez un câble série à brochage direct (RS-232) pour relier un modem série externe au port libellé MODEM à l'arrière de LX. Reportez-vous à Spécifications pour obtenir la liste des modems agréés et à ***Configuration des paramètres de modem*** (à la page 144) pour plus d'informations sur la configuration du modem.

Remarque : Raritan recommande de configurer le modem en activant le paramètre CD (carrier detect).

Etape 4 : Configuration de LX

A la première mise sous tension du dispositif LX, vous devez effectuer des opérations de configuration initiale via la console locale de LX :

- Modifier le mot de passe par défaut
- Affecter l'adresse IP
- Désigner les serveurs cible KVM

LX est configurable à distance via un navigateur Web. Votre poste de travail doit donc disposer d'une version de Java Runtime Environment (JRE) appropriée.

Modification du mot de passe par défaut

LX est livré avec un mot de passe par défaut. La première fois que vous démarrez l'unité, il vous est demandé de changer ce mot de passe.

Pour changer le mot de passe par défaut :

1. Une fois l'unité amorcée, entrez le nom d'utilisateur (admin) et le mot de passe (raritan) par défaut. Cliquez sur Login (Se connecter).
2. Entrez l'ancien mot de passe (raritan), le nouveau mot de passe, puis encore le nouveau. Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques et caractères spéciaux (présents sur un clavier anglais). Cliquez sur Apply (Appliquer). Cliquez sur OK sur la page Confirmation.

Remarque : le mot de passe par défaut peut également être modifié à partir de Multi-Platform Client (MPC) de Raritan.

Affectation d'une adresse IP

Ces procédures décrivent comment affecter une adresse IP sur la page Network Settings (Paramètres réseau). Pour obtenir des informations complètes sur tous les champs ainsi que sur le fonctionnement de cette page, reportez-vous à ***Paramètres réseau*** (à la page 132).

Pour affecter une adresse IP :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Indiquez un nom de dispositif significatif pour votre unité LX. 32 caractères alphanumériques au plus, avec des caractères spéciaux valides et aucun espace.
3. Dans la section IPv4, entrez ou sélectionnez les paramètres réseau spécifiques à IPv4 appropriés :

a. Entrez l'adresse IP si nécessaire. L'adresse IP par défaut est 192.168.0.192.

b. Entrez le masque de sous-réseau. Le masque de sous-réseau par défaut est 255.255.255.0.

c. Entrez la passerelle par défaut si None (Néant) est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).

d. Entrez le nom d'hôte DHCP préféré si DHCP est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).

e. Sélectionnez la configuration IP automatique. Les options suivantes sont disponibles :

- None (Static IP) (Néant (IP statique)) : cette option nécessite que vous indiquiez manuellement les paramètres réseau.

  Cette option est recommandée car LX est un dispositif d'infrastructure et son adresse IP ne doit pas être modifiée.

- DHCP : le protocole de configuration d'hôte dynamique est utilisé par les ordinateurs mis en réseau (clients) pour obtenir des adresses IP uniques et d'autres paramètres à partir du serveur DHCP.

  Avec cette option, les paramètres réseau sont attribués par le serveur DHCP. Si DHCP est utilisé, entrez le nom d'hôte préféré (DHCP uniquement). Maximum de 63 caractères.

4. Si IPv6 doit être utilisé, entrez ou sélectionnez les paramètres réseau spécifiques à IPv6 appropriés dans la section IPv6 :

   a. Cochez la case IPv6 pour activer les champs de la section.

   b. Renseignez le champ Global/Unique IP Address (Adresse IP globale/unique). Il s'agit de l'adresse IP affectée à LX.

   c. Renseignez le champ Prefix Length (Longueur de préfixe). Il s'agit du nombre de bits utilisés dans l'adresse IPv6.

   d. Renseignez le champ Gateway IP Address (Adresse IP de la passerelle).

   e. Link-Local IP Address (Adresse IP Lien-local). Cette adresse est attribuée automatiquement au dispositif. Elle est utilisée pour la détection de voisins ou en l'absence de routeurs. **Read-Only (Lecture seule)**

   f. Zone ID. Ce champ identifie le dispositif auquel l'adresse est associée. **Read-Only (Lecture seule)**

   g. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :

- None (Néant) - Utilisez cette option si vous ne souhaitez pas de configuration IP automatique et préférez définir l'adresse IP vous-même (IP statique). Cette option par défaut est recommandée.

  Lorsqu'elle est sélectionnée pour la configuration IP automatique, les champs Network Basic Settings (Paramètres réseau de base) sont activés : Global/Unique IP Address (Adresse IP globale/unique), Prefix Length (Longueur de préfixe) et Gateway IP Address (Adresse IP de la passerelle). Vous pouvez paramétrer manuellement la configuration IP.

- Router Discovery (Détection de routeur) - Utilisez cette option pour affecter automatiquement des adresses IPv6 ayant une portée « Global » ou « Unique Local » au-delà des adresses « Link Local » qui ne s'appliquent qu'à un sous-réseau connecté directement.

5. Sélectionnez Obtain DNS Server Address Automatically (Obtenir l'adresse du serveur DNS automatiquement) si DHCP est sélectionné et que l'option Obtain DNS Server Address (Obtenir l'adresse du serveur DNS) est activée. Si l'option When Obtain DNS Server Address Automatically est sélectionnée, les données DNS fournies par le serveur DHCP seront utilisées.
6. Si l'option Use the Following DNS Server Addresses (Utiliser les adresses de serveur DNS suivantes) est sélectionnée, indépendamment de la sélection de DHCP ou non, les adresses entrées dans cette section seront utilisées pour la connexion au serveur DNS.

   Entrez les données suivantes si l'option Use the Following DNS Server Addresses est sélectionnée. Il s'agit des adresses DNS principale et secondaire qui seront utilisées si la connexion au serveur DNS principal est perdue en raison d'une panne.

   a. Primary DNS Server IP Address (Adresse IP du serveur DNS principal)
   b. Secondary DNS Server IP Address (Adresse IP du serveur DNS secondaire)
7. Lorsque vous avez terminé, cliquez sur OK.

Reportez-vous à Paramètres de l'interface LAN pour plus d'informations sur la configuration de cette section de la page Network Settings (Paramètres réseau).

Remarque : dans certains environnements, le paramètre par défaut du champ LAN Interface Speed & Duplex (Vitesse d'interface LAN & Duplex), Autodetect (auto-détection), ne définit pas correctement les paramètres réseau, ce qui entraîne des problèmes sur le réseau. Dans ce cas, paramétrez le champ LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN) de LX sur 100 Mbps/Full Duplex (Bidirectionnel simultané) (ou toute option appropriée à votre réseau) pour résoudre le problème. Reportez-vous à la page **Paramètres réseau** *(à la page 132) pour plus d'informations.*

Configuration des paramètres de date et heure (facultatif)

▶ Pour définir la date et l'heure :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Date/Time (Date/heure). La page Date/Time Settings (Paramètres de date/heure) s'ouvre.
2. Sélectionnez votre fuseau horaire dans la liste déroulante Time Zone (Fuseau horaire).
3. Pour prendre en compte l'heure d'été, cochez la case Adjust for daylight savings time (Régler selon les changements d'heure).
4. Choisissez la méthode que vous souhaitez utiliser pour définir la date et l'heure :
   - User Specified Time - Sélectionnez cette option pour saisir la date et l'heure manuellement. Pour l'option User Specified Time (Heure spécifiée par l'utilisateur), entrez la date et l'heure. Pour l'heure, utilisez le format hh:mm (système de 24 heures).
   - Synchronize with NTP Server - Sélectionnez cette option pour synchroniser la date et l'heure avec le serveur NTP.
5. Pour l'option Synchronize with NTP Server (Synchroniser avec le serveur NTP) :
   a. Entrez une adresse IP dans le champ Primary Time server (Serveur d'horloge principal).
   b. Renseignez le champ Secondary Time server (Serveur d'horloge secondaire). **Facultatif**
6. Cliquez sur OK.

Désignation des serveurs cible

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait. Reportez-vous à **Etape 3 : Connexion de l'équipement** pour obtenir une description de la connexion de l'équipement.
2. A l'aide de la console locale LX, choisissez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports), cliquez sur le nom du port du serveur cible à nommer.
3. Entrez le nom du serveur, qui peut comporter jusqu'à 32 caractères alphanumériques et spéciaux. Cliquez sur OK.

Caractères spéciaux valides pour les noms de cibles

<table>
<tr><th>Caractère</th><th>Description</th><th>Caractère</th><th>Description</th></tr>
<tr><td>!</td><td>Point d'exclamation</td><td>;</td><td>Point-virgule</td></tr>
<tr><td>"</td><td>Guillemet</td><td>=</td><td>Signe égal</td></tr>
<tr><td>#</td><td>Dièse</td><td>></td><td>Signe supérieur à</td></tr>
<tr><td>$</td><td>Symbole du dollar</td><td>?</td><td>Point d'interrogation</td></tr>
<tr><td>%</td><td>Symbole du pourcentage</td><td>@</td><td>Arobas</td></tr>
<tr><td>&</td><td>« Et » commercial</td><td>[</td><td>Crochet ouvrant</td></tr>
<tr><td>(</td><td>Parenthèse ouvrante</td><td>\</td><td>Trait oblique inversé</td></tr>
<tr><td>)</td><td>Parenthèse fermante</td><td>]</td><td>Crochet fermant</td></tr>
<tr><td>*</td><td>Astérisque</td><td>^</td><td>Accent circonflexe</td></tr>
<tr><td>+</td><td>Signe plus</td><td>_</td><td>Trait de soulignement</td></tr>
<tr><td>,</td><td>Virgule</td><td>`</td><td>Accent grave</td></tr>
<tr><td>-</td><td>Tiret</td><td>{</td><td>Accolade gauche</td></tr>
<tr><td>.</td><td>Point</td><td>|</td><td>Barre</td></tr>
<tr><td>/</td><td>Trait oblique</td><td>}</td><td>Accolade droite</td></tr>
<tr><td><</td><td>Signe inférieur à</td><td>~</td><td>Tilde</td></tr>
<tr><td>:</td><td>Deux-points</td><td></td><td></td></tr>
</table>

Authentification à distance

Protocoles pris en charge

Afin de simplifier la gestion des noms d'utilisateur et des mots de passe, LX offre la possibilité de transférer les requêtes d'authentification vers un serveur d'authentification externe. Deux protocoles d'authentification externes sont pris en charge : LDAP/LDAPS et RADIUS.

Remarque relative à Microsoft Active Directory

Microsoft® Active Directory® utilise le protocole LDAP/LDAPS de manière native et peut servir de source d'authentification et serveur LDAP/LDAPS avec LX. Si le serveur Microsoft Active Directory dispose d'un composant IAS (serveur d'autorisation Internet), il peut également être utilisé comme source d'authentification RADIUS.

Création de groupes d'utilisateurs et d'utilisateurs

Dans le cadre de la configuration initiale, vous devez définir des groupes d'utilisateurs et des utilisateurs pour permettre à ces derniers d'accéder à LX.

Outre les groupes par défaut fournis par le système, vous pouvez aussi créer des groupes et spécifier les autorisations adéquates pour répondre à vos besoins.

Un nom d'utilisateur et un mot de passe sont nécessaires pour accéder à LX. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre LX. Reportez-vous à **Gestion des utilisateurs (à la page 108) pour plus d'informations sur l'ajout et la modification des groupes d'utilisateurs et des utilisateurs.**

Etape 5 : Lancement de la console distante de LX

Pour démarrer la console distante de LX :

1. Connectez-vous à un poste de travail doté d'une connectivité réseau à votre dispositif LX, et de Microsoft .NET® et/ou Java Runtime Environment® (JRE® est disponible sur le ***site Web de Java http://java.sun.com/***).
2. Démarrez un navigateur Web pris en charge, tel qu'Internet Explorer® ou Firefox®.
3. Entrez l'URL : *http://ADRESSE-IP* ou *http://ADRESSE-IP/akc* pour .NET, où ADRESSE-IP est l'adresse IP affectée à LX. Vous pouvez aussi utiliser https, le nom DNS de LX attribué par l'administrateur (à condition qu'un serveur DNS ait été configuré), ou saisir l'adresse IP dans le navigateur (LX redirige toujours l'adresse IP de HTTP vers HTTPS).

4. Entrez vos nom d'utilisateur et mot de passe. Cliquez sur Login (Se connecter).

Accès et gestion des serveurs cible à distance

La page Port Access (Accès aux ports) de LX fournit la liste de tous les ports du produit, des serveurs cible connectés, de leur état et de leur disponibilité.

Accès à un serveur cible

▶ **Pour accéder à un serveur cible :**

1. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu d'action des ports apparaît.
2. Sélectionnez Connect (Connecter) dans le menu d'action des ports. Une fenêtre KVM s'ouvre, qui contient une connexion à la cible.

Commutation entre les serveurs cible

▶ **Pour commuter entre des serveurs cible KVM :**

1. Si vous utilisez déjà un serveur cible, accédez à la page Port Access de LX.
2. Cliquez sur le nom du port associé à la cible à laquelle vous souhaitez accéder. Le menu Port Action (Action des ports) apparaît.
3. Sélectionnez Switch From (Commuter depuis) dans le menu d'action des ports. Le nouveau serveur cible sélectionné est affiché.

Déconnexion d'un serveur cible

▶ **Pour déconnecter un serveur cible :**

- Cliquez sur le nom de port de la cible que vous souhaitez déconnecter. Lorsque le menu Port Action (Action des ports) apparaît, cliquez sur Disconnect (Déconnecter).

Etape 6 : Configuration de la langue du clavier (facultatif)

Remarque : cette étape n'est pas obligatoire si vous utilisez un clavier américain/international.

Si vous utilisez une langue autre que l'anglais américain, le clavier doit être configuré pour celle-ci. De plus, la langue du clavier de l'ordinateur client et des serveurs cible KVM doit être la même.

Consultez la documentation de votre système d'exploitation pour plus d'informations sur la modification de la disposition du clavier.

Modification du code de disposition de clavier (cibles Sun)

Suivez cette procédure si vous disposez d'un DCIM-SUSB et souhaitez utiliser une disposition de clavier dans une autre langue.

- **Pour modifier le code de disposition du clavier (DCIM-SUSB uniquement) :**

1. Ouvrez une fenêtre de l'éditeur de texte sur le poste de travail Sun™.
2. Assurez-vous que la touche Verr num est active, et appuyez sur la touche Ctrl située à gauche et sur la touche Suppr du clavier. Le voyant du verrouillage des majuscules clignote pour indiquer que le CIM est en mode de modification du code de disposition. La fenêtre de texte affiche les informations suivantes : `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX).`
3. Saisissez le code de disposition souhaité (par exemple, *31* pour le clavier japonais).
4. Appuyez sur Entrée.
5. Mettez le dispositif hors tension, puis à nouveau sous tension. Le DCIM-SUSB procède à une réinitialisation (alimentation cyclique).
6. Vérifiez que les caractères sont corrects.

Etape 7 : Configuration de la fonction multiniveau (facultatif)

LX et la fonction multiniveau générique sont pris en charge par LX. Reportez-vous à la section **Gestion des dispositifs** (à la page 132) pour plus d'informations sur cette fonction.

Connectez depuis un port de serveur cible sur le dispositif de base aux ports vidéo/clavier/souris du port Local Access du LX en niveau à l'aide d'un D2CIM-DVUSB.

- **Pour activer la fonction multiniveau :**

1. Depuis la base du niveau, choisissez Device Settings > Device Services (Paramètres du dispositif > Services du dispositif). La page de paramétrage Device Services (Services du dispositif) apparaît.
2. Sélectionnez Enable Tiering as Base (Activer la fonction multiniveau comme base).
3. Dans le champ Base Secret (Secret de la base), entrez le secret partagé entre la base et les dispositifs en niveau. Ce secret est exigé pour permettre aux dispositifs en niveau d'authentifier le dispositif de base. Vous entrerez le même mot secret pour le dispositif en niveau.
4. Cliquez sur OK.
5. Activez les dispositifs en niveau. Depuis le dispositif en niveau, choisissez Device Settings > Local Port Settings (Paramètres du dispositif > Paramètres du port local).

6. Dans la section Enable Local Ports (Activer les ports locaux) de la page, sélectionnez Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local).
7. Dans le champ Tier Secret (Secret du niveau), entrez le mot secret entré pour le dispositif de base sur la page Device Settings (Paramètres du dispositif).
8. Cliquez sur OK.

Chapitre 3 Utilisation des serveurs cible

Dans ce chapitre

Interfaces LX

LX dispose de plusieurs interfaces utilisateur qui fournissent un accès aisé aux cibles à tout moment, où que vous soyez. Ces interfaces incluent la console locale de LX, la console distante de LX, Virtual KVM Client (VKC), Active KVM Client (AKC) et Multi-Platform Client (MPC). Le tableau ci-après décrit les interfaces et leur utilisation pour l'accès aux serveurs cible et la gestion de ces derniers localement et à distance :

Interface utilisateur	Locale		Distante	
	distant	Admin	distant	Admin
Console locale de LX	✓	✓		
Console distante de LX			✓	✓
Virtual KVM Client (VKC)			✓	
Multi-Platform Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

Les sections suivantes de l'aide contiennent des informations sur l'utilisation d'interfaces particulières pour accéder à LX et gérer les cibles :

- Console locale
- Console distante
- Virtual KVM Client
- Multi-Platform Client

Interface de la console locale de LX : Dispositifs LX

Lorsque vous êtes situé au niveau du rack du serveur, LX permet une gestion KVM standard via la console locale de LX. La console locale de LX offre une connexion (analogique) KVM directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur.

Les interfaces graphiques utilisateur de la console locale de LX et de la console distante de LX présentent de nombreuses ressemblances. Les éventuelles différences sont indiquées dans l'aide.

L'option Factory Reset (Rétablir les valeurs usine) est disponible sur la console locale de LX et non sur la console distante de LX.

Interface de la console distante de LX

La console distante de LX est une interface graphique utilisateur navigateur qui vous permet de vous connecter aux serveurs cible KVM et aux cibles série connectés à LX, et de gérer LX à distance.

Elle offre une connexion numérique à vos serveurs cible KVM connectés. Lorsque vous accédez à un serveur cible KVM à l'aide de la console distante de LX, une fenêtre Virtual KVM Client s'ouvre.

Il existe de nombreuses ressemblances entre les interfaces utilisateur graphiques de la console locale de LX et de la console distante de LX. Les éventuelles différences sont indiquées dans le manuel d'utilisation. Les options suivantes sont disponibles sur la console distante de LX mais non sur la console locale de LX :

- Support virtuel
- Favorites (Favoris)
- Backup/Restore (Sauvegarde/Restauration)
- Firmware Upgrade (Mise à niveau du firmware)
- Certificats SSL

Lancement de la console distante de LX

Important : quel que soit le navigateur utilisé, vous devez autoriser les fenêtres contextuelles provenant de l'adresse IP du dispositif pour lancer la console distante de LX.

Selon le navigateur utilisé et les paramètres de sécurité, il est possible que plusieurs avertissements relatifs aux certificats et à la sécurité s'affichent. Il vous faudra accepter ces avertissements pour lancer la console distante de LX.

Vous pouvez réduire le nombre de messages d'avertissement lors des connexions suivantes en cochant les options suivantes dans les messages d'avertissement relatifs aux certificats et à la sécurité :

- In the future, do not show this warning (A l'avenir, ne plus afficher ce message d'avertissement)
- Always trust content from this publisher (Toujours faire confiance au contenu provenant de cet éditeur)

Pour démarrer la console distante de LX :

1. Connectez-vous à un poste de travail doté d'une connectivité réseau à votre dispositif LX, et de Microsoft .NET® et/ou Java Runtime Environment® (JRE® est disponible sur le ***site Web de Java http://java.sun.com/***).
2. Démarrez un navigateur Web pris en charge, tel qu'Internet Explorer® ou Firefox®.
3. Entrez l'URL : *http://ADRESSE-IP* ou *http://ADRESSE-IP/akc* pour .NET, où ADRESSE-IP est l'adresse IP affectée à LX. Vous pouvez aussi utiliser https, le nom DNS de LX attribué par l'administrateur (à condition qu'un serveur DNS ait été configuré), ou saisir l'adresse IP dans le navigateur (LX redirige toujours l'adresse IP de HTTP vers HTTPS).
4. Tapez votre nom d'utilisateur et votre mot de passe. S'il s'agit de la première connexion, utilisez le nom d'utilisateur (admin) et le mot de passe (raritan, en minuscules) par défaut usine. Il vous est alors demandé de modifier le mot de passe par défaut. Cliquez sur Login (Se connecter).

Reportez-vous à ***Virtual KVM Client (VKC) et Active KVM Client (AKC)*** (à la page 59) pour plus d'informations sur les fonctions LX disponibles via la console distante.

Interface et navigation

Interface LX

Les interfaces des consoles distante et locale de LX présentent toutes les deux une interface Web pour la configuration et l'administration de dispositifs, ainsi qu'une liste et des fonctions de sélection des serveurs cible. Les options sont organisées dans différents onglets.

Une fois la connexion réussie, la page d'accès aux ports s'affiche avec la liste de tous les ports ainsi que leur statut et leur disponibilité. Deux onglets figurent sur la page, View by Port (Vue par port) et Set Scan (Balayage d'ensemble). Sur l'onglet View by Port, vous pouvez effectuer un tri par numéro de port, nom de port, statut (activé ou non) et disponibilité (inactif, connecté, occupé, indisponible ou en cours de connexion) en cliquant sur l'en-tête de colonne. Pour modifier le nombre de ports affichés sur la page, entrez un nombre dans le champ Rows per Page (Lignes par page) dans le coin inférieur droit de la page et cliquez sur Set (Définir). Reportez-vous à ***Page Port Access*** (à la page 47) pour plus d'informations.

Utilisez l'onglet Set Scan (Balayage d'ensemble) pour effectuer le balayage des 32 cibles au maximum connectées à LX. Reportez-vous à ***Balayage des ports*** (à la page 50).

Panneau gauche

Le panneau gauche de l'interface LX contient les informations suivantes. Notez que certaines d'entre elles sont conditionnelles et ne s'afficheront que si vous êtes un utilisateur particulier, utilisez certaines fonctions, etc. Les informations conditionnelles sont indiquées ici.

Information	Description	Affichée quand ?
Time & Session (Heure & session)	Date et heure de début de la session en cours.	Toujours
Utilisateur	Nom d'utilisateur	Toujours
State (Etat)	Etat actuel de l'application, inactive ou active. Si l'application est active, elle suit et affiche la durée d'inactivité de la session.	Toujours
Your IP (Votre IP)	Adresse IP utilisée pour accéder à LX.	Toujours
Last Login (Dernière connexion)	Date et heure de la dernière connexion.	Toujours
Device Information (Informations sur le dispositif)	Information spécifique au LX que vous utilisez.	Toujours
Device Name (Nom du dispositif)	Nom affecté au dispositif.	Toujours
IP Address (Adresse IP)	Adresse IP du LX.	Toujours
Firmware	Version actuelle du firmware.	Toujours
Device Model (Modèle du dispositif)	Modèle du LX	Toujours
Configured As Base or Configured As Tiered* (Configuré comme base ou Configuré comme niveau)	Si vous utilisez une configuration multiniveau, ceci indique si le LX auquel vous accédez est le dispositif de base ou un dispositif en niveau.	Lorsque LX fait partie d'une configuration multiniveau

Information	Description	Affichée quand ?
Port States (Etats des ports)	Statut des ports utilisés par LX.	Toujours
Utilisateurs connectés	Utilisateurs, identifiés par leur nom d'utilisateur et adresse IP, actuellement connectés au LX.	Toujours
Aide en ligne	Liens vers l'aide en ligne.	Toujours
Favorite Devices (Dispositifs favoris)	Reportez-vous à ***Gestion des favoris*** (à la page 53).	Toujours

Navigation dans la console LX

Les interfaces de la console LX offrent plusieurs méthodes de navigation et de sélection.

Pour sélectionner une option (utilisez n'importe laquelle des méthodes suivantes) :

- Cliquez sur un onglet. Une page d'options disponibles apparaît.
- Placez le curseur sur un onglet puis sélectionnez l'option souhaitée dans le menu.
- Cliquez sur l'option directement dans la hiérarchie de menu affichée (fils d'Ariane).

Pour faire défiler les pages plus longues que l'écran :

- Utilisez les touches PageSup et PageInf sur votre clavier ;
- utilisez la barre de défilement à droite de l'écran.

Page Port Access

Une fois connecté à la console distante de LX, la page Port Access (Accès aux ports) s'ouvre. Par défaut, l'onglet View by Port (Afficher par port) apparaît sur la page Port Access. Elle répertorie tous les ports de LX, les serveurs cible KVM connectés ainsi que leur état et leur disponibilité. Elle indique le chemin permettant d'accéder aux serveurs cible KVM connectés à LX. Ces serveurs cible KVM sont des serveurs que vous souhaitez gérer via le dispositif LX. Ils sont connectés aux ports de LX placés à l'arrière du dispositif.

Remarque : une nouvelle fenêtre Virtual KVM Client s'ouvre pour chaque connexion à un serveur KVM cible.

Si vous utilisez une configuration multiniveau où un dispositif LX de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, vous pouvez afficher les dispositifs en niveau sur la page Port Access (Accès aux ports) en cliquant sur l'icône Expand Arrow ▶ (flèche de développement) à gauche du nom du dispositif en niveau. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.

La fonction de balayage des ports est accessible depuis l'onglet Set Scan (Balayage d'ensemble) de la page Port Access (Accès aux ports). Elle vous permet de définir un ensemble de cibles à balayer. Des vues en miniature des cibles balayées sont également disponibles. Sélectionnez une miniature pour ouvrir la cible correspondante dans sa fenêtre Virtual KVM Client.

▶ Pour utiliser la page Port Access :

1. Dans la console distante de LX, cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche.

   Les serveurs cible KVM sont triés initialement par numéro de port. Vous pouvez modifier l'affichage en effectuant le tri sur n'importe quelle colonne.

   - Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif LX.
   - Port Name (Nom de port) - Nom du port de LX. Initialement, ce champ est défini sur Dominion-LX-Port# mais vous pouvez remplacer ce nom par un autre plus parlant. Lorsque vous cliquez sur un lien Port Name (Nom du port), le menu d'action des ports (Port Action Menu) s'affiche.

Remarque : n'utilisez pas d'apostrophe pour le nom de port (CIM).

   - Type - Type de serveur ou CIM.
   - Status (Statut) - Le statut des serveurs cible standard est activé ou désactivé.

- Availability (Disponibilité) - La disponibilité du serveur.

2. Cliquez sur le nom du port du serveur cible auquel vous souhaitez accéder. Le menu d'action des ports (Port Action Menu) apparaît. Reportez-vous à Port Action Menu (Menu d'action de ports) pour plus d'informations sur les options de menu disponibles.
3. Sélectionnez la commande souhaitée dans le menu d'action des ports.
4. Définissez un ensemble de ports à balayer sur LX à l'aide de la fonction Set Scan (Balayage d'ensemble). Reportez-vous à ***Balayage des ports*** (à la page 50).

Pour modifier l'ordre de tri et/ou afficher des ports supplémentaires sur la même page :

1. Cliquez sur l'en-tête de la colonne par laquelle vous souhaitez effectuer un tri. La liste des serveurs cible KVM est triée par cette colonne.
2. Dans Rows per Page (Lignes par page), entrez le nombre de ports à afficher sur la page et cliquez sur Set (Définir).

Port Action Menu (Menu d'action de ports)

Lorsque vous cliquez sur un nom de port dans la liste Port Access, le menu d'action des ports s'affiche. Choisissez l'option de menu souhaitée pour ce port afin de l'exécuter. Notez que seules les options actuellement disponibles, suivant l'état et la disponibilité du port, sont répertoriées dans le menu d'actions des ports :

- Connect (Connecter) - Crée une nouvelle connexion au serveur cible. Pour la console distante de LX, une nouvelle page Virtual KVM Client apparaît. Pour la console locale de LX, l'affichage passe de l'interface utilisateur locale au serveur cible. Sur le port local, l'interface de la console locale de LX doit être visible pour pouvoir procéder à la commutation. La commutation par raccourci-clavier est également disponible à partir du port local.

  Remarque : cette option n'apparaît pas pour un port disponible à partir de la console distante LX si toutes les connexions sont occupées.

- Switch From (Basculer depuis) : permet de basculer d'une connexion existante au port sélectionné (serveur cible KVM). Cette option de menu n'est disponible que pour les cibles KVM. Elle n'est visible que si un client KVM virtuel est ouvert.

  Remarque : cette option de menu n'est pas disponible sur la console locale de LX.

- Disconnect : déconnecte ce port et ferme la page du client virtuel KVM correspondant à ce serveur cible. Cette option de menu est disponible uniquement lorsque l'état du port est actif et connecté, ou actif et occupé.

Remarque : cette option de menu n'est pas disponible sur la console locale de LX. La seule façon de se déconnecter de la cible activée dans la console locale est d'utiliser le raccourci clavier.

Balayage des ports

LX offre une fonction de balayage des ports qui recherche les cibles sélectionnées et les affiche dans une vue en diaporama, ce qui vous permet de contrôler jusqu'à 32 cibles simultanément. Vous pouvez vous connecter aux cibles ou sélectionner une cible spécifique le cas échéant. Les balayages peuvent inclure des cibles standard, des dispositifs Dominion en niveau et des ports de commutateurs KVM.

Remarque : le balayage des dispositifs en niveau n'est pas pris en charge par Multi-Platform Client (MPC).

Lorsque vous démarrez un balayage, la fenêtre Port Scan (Balayage des ports) s'ouvre. Au fur et à mesure de la détection d'une cible, celle-ci est affichée sous forme de miniature dans un diaporama. Le diaporama parcourt les miniatures des cibles selon l'intervalle par défaut de 10 secondes ou par l'intervalle que vous indiquez. Au fur et à mesure du balayage des cibles, celle qui est sélectionnée dans le diaporama s'affiche au centre de la page. Reportez-vous à ***Paramètres de balayage*** (à la page 89).

Vous pouvez modifier le délai de rotation des miniatures dans le diaporama, l'intervalle de sélection d'une miniature et les paramètres d'affichage de la page dans l'onglet Scan Settings (Paramètres de balayage) de la boîte de dialogue Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC) Tools > Options (Outils VKC, AKC et MPC > Options). Reportez-vous à ***Paramètres de balayage*** (à la page 89).

Le nom de la cible s'affiche sous sa miniature et dans la barre de tâches au bas de la fenêtre. Si une cible est occupée, un écran vide apparaît au lieu de la page d'accès au serveur cible.

Le statut de chaque cible est indiqué par des voyants vert, jaune et rouge affichés sous la miniature de la cible, et lorsque la cible est sélectionnée dans la rotation, dans la barre de tâches. Les voyants indiquent les statuts suivants :

- Vert : la cible est activée/inactive ou activée/connectée.
- Jaune : la cible est désactivée mais connectée.
- Rouge : la cible est désactivée/inactive, occupée ou non accessible.

Cette fonction est disponible depuis le port local, Virtual KVM Client (VKC), Active KVM Client (AKC) et Multi-Platform Client (MPC).

Remarque : MPC utilise une méthode différente des autres clients Raritan pour déclencher un balayage. Reportez-vous à ***Set Scan Group*** *(Groupe de balayage d'ensemble) dans le* ***guide des clients KVM et série*** *pour plus d'informations. Les résultats et les options de balayage de la console distante et de la console locale sont différents. Reportez-vous à* **Balayage des ports - Console locale** *(à la page 201).*

▶ Pour effectuer le balayage de cibles :

1. Cliquez sur l'onglet Set Scan (Balayage d'ensemble) dans la page Port Access (Accès aux ports).
2. Sélectionnez les cibles à inclure au balayage en cochant la case située à gauche de chacune, ou cochez la case au sommet de la colonne des cibles pour les sélectionner toutes.
3. Laissez la case Up Only (Activées seulement) cochée si vous ne souhaitez inclure au balayage que les cibles activées. Décochez-la pour inclure toutes les cibles, activées ou désactivées.
4. Cliquez sur Scan (Balayer) pour démarrer le balayage. Au fur et à mesure du balayage, chaque cible est affiché dans la vue en diaporama de la page.
5. Cliquez sur Options > Pause pour interrompre le diaporama et arrêter son mouvement entre les cibles. Cliquez sur Options > Resume (Reprendre) pour reprendre le diaporama.
6. Cliquez sur une miniature de cible pour procéder à son balayage.
7. Connectez-vous à une cible en double-cliquant sur sa miniature.

View By Port | Set Scan

▲ No.	Name	Type	Status	Availability
1	Dominion_LX_Port1	Not Available	down	idle
2	Dominion_LX_Port2	Not Available	down	idle
3	Dominion_LX_Port3	Not Available	down	idle
4	Dominion_LX_Port4	Not Available	down	idle
5	Dominion_LX_Port5	Not Available	down	idle
6	Dominion_LX_Port6	Not Available	down	idle
7	Dominion_LX_Port7	Not Available	down	idle
8	Dominion_LX_Port8	Not Available	down	idle
9	Dominion_LX_Port9	Not Available	down	idle
10	[illegible]	[illegible]	[illegible]	idle

Utilisation des options de balayage

Les options suivantes sont disponibles pour le balayage des cibles. A l'exception de l'icône Expand/Collapse (Développer/Réduire), toutes ces options sont sélectionnées à partir du menu Options en haut à gauche de l'afficheur Port Scan (Balayage des ports). Les valeurs par défaut des options sont rétablies lorsque vous fermez la fenêtre.

Masquer ou afficher les miniatures

- Utilisez l'icône Expand/Collapse (Développer/Réduire) en haut à gauche de la fenêtre pour masquer ou afficher les miniatures. Par défaut, la vue est développée.

Interrompre le diaporama des miniatures

- Pour interrompre la rotation des miniatures entre deux cibles, sélectionnez Options > Pause. La rotation des miniatures est le paramètre par défaut.

Reprendre le diaporama des miniatures

- Pour reprendre la rotation des miniatures, sélectionnez Options > Resume (Reprendre).

Dimensionner les miniatures dans l'afficheur Port Scan (Balayage des ports)

- Pour agrandir les miniatures, sélectionnez Options > Size (Taille) > 360x240.
- Pour réduire les miniatures, sélectionnez Options > Size (Taille) > 160x120. Il s'agit de la taille par défaut des miniatures.

Modifier l'orientation de l'afficheur Port Scan (Balayage des ports)

- Pour afficher les miniatures le long du bas de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Horizontal.
- Pour afficher les miniatures le long du côté droit de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Vertical. Il s'agit de la vue par défaut.

Gestion des favoris

Une fonction Favorites (Favoris) intégrée permet d'organiser les dispositifs que vous utilisez fréquemment et d'y accéder rapidement. La section Favorite Devices (Dispositifs favoris) se trouve dans la partie inférieure gauche (cadre) de la page Port Access et permet les opérations suivantes :

- créer et gérer une liste de dispositifs favoris ;
- accéder rapidement aux dispositifs fréquemment utilisés ;
- répertorier vos favoris par nom de dispositif, adresse IP ou nom d'hôte DNS ;
- détecter les dispositifs LX sur le sous-réseau (avant et après la connexion) ;
- récupérer les dispositifs LX détectés à partir du dispositif Dominion connecté (après la connexion).

▶ Pour accéder à un dispositif LX favori :

- Cliquez sur le nom du dispositif (liste figurant sous Favorite Devices). Un nouveau navigateur s'ouvre pour le dispositif en question.

▶ Pour afficher les favoris en fonction de leur nom :

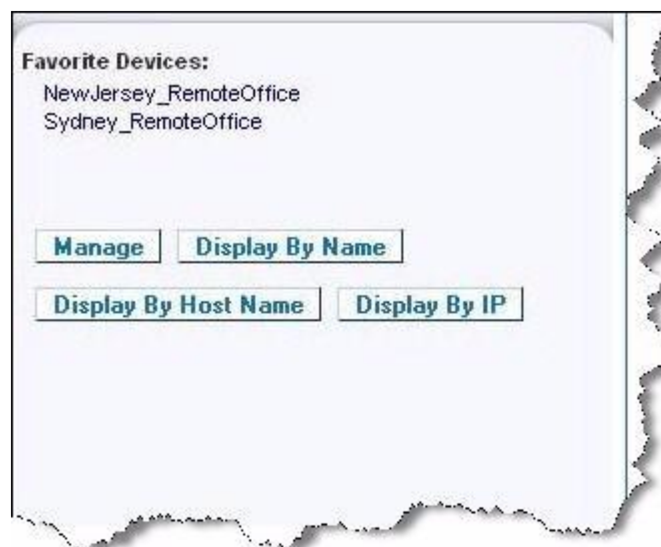
- Cliquez sur Display by Name (Afficher par nom).

▶ Pour afficher les favoris en fonction de leur adresse IP :

- Cliquez sur Display by IP (Afficher par adresse IP).

▶ Pour afficher les favoris en fonction du nom d'hôte :

- Cliquez sur Display by Host Name (Afficher par nom d'hôte).



Page Manage Favorites (Gérer les favoris)

Pour ouvrir la page Manage Favorites :

- Cliquez sur Manage (Gérer) dans le panneau de gauche. La page Manage Favorites (Gérer les favoris) qui s'ouvre contient les éléments suivants :

Utilisez :	Pour :
Liste des favoris (Favorites List)	Gérer la liste de vos dispositifs favoris.
Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local)	Détecter les dispositifs Raritan sur le sous-réseau local du PC client.
Discover Devices - LX Subnet (Détecter les dispositifs - Sous-réseau de LX)	Détecter les dispositifs Raritan sur le sous-réseau du dispositif LX.
Add New Device to Favorites (Ajouter un nouveau dispositif aux favoris)	Ajouter, modifier et supprimer des dispositifs dans votre liste de favoris.

Page Favorites List (Liste des favoris)

A partir de la page Favorites List, vous pouvez ajouter, modifier et supprimer des dispositifs dans votre liste de favoris.

Pour ouvrir la page Favorites List :

- Sélectionnez Manage (Gérer) > Favorites List (Liste des favoris). La page Favorites List s'ouvre.

Détection des dispositifs sur le sous-réseau local

Cette option détecte les dispositifs sur votre sous-réseau local, c'est-à-dire le sous-réseau sur lequel la console distante de LX est exécutée. Ces dispositifs sont accessibles directement à partir de cette page ou vous pouvez les ajouter à votre liste de favoris. Reportez-vous à ***Page Favorites List (Liste des favoris)*** (à la page 54).

Pour détecter des dispositifs sur le sous-réseau local :

1. Sélectionnez Manage (Gérer) > Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local). La page Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local) apparaît.
2. Choisissez le port de détection approprié :
   - Pour utiliser le port de détection par défaut, sélectionnez la case Use Default Port 5000 (Utiliser le port 5000 par défaut).
   - Pour utiliser un port de détection différent :
   a. Désélectionnez la case Use Default Port 5000 (Utiliser le port 5000 par défaut).
   b. Entrez le numéro de port dans le champ Discover on Port (Détecter sur le port).
   c. Cliquez sur Save (Enregistrer).
3. Cliquez sur Refresh (Actualiser). La liste des dispositifs du sous-réseau KX est actualisée.

Pour ajouter des dispositifs à votre liste de favoris :

1. Cochez la case située en regard du nom du dispositif/de l'adresse IP.
2. Cliquez sur Add (Ajouter).

Pour accéder à un dispositif détecté :

- Cliquez sur le nom du dispositif ou sur son adresse IP. Un nouveau navigateur s'ouvre pour le dispositif en question.

Détection des dispositifs sur le sous-réseau de LX

Cette option détecte les dispositifs sur le sous-réseau du dispositif, c'est-à-dire le sous-réseau de l'adresse IP du dispositif LX même. Vous pouvez accéder à ces dispositifs directement à partir de la page Subnet (Sous-réseau) ou les ajouter à votre liste de favoris. Reportez-vous à ***Page Favorites List (Liste des favoris)*** (à la page 54).

Cette fonction permet à plusieurs dispositifs LX d'interagir et de se mettre en corrélation automatiquement. La console distante de LX détecte automatiquement les dispositifs LX, et n'importe quel autre dispositif Raritan, sur le sous-réseau de LX.

Pour détecter des dispositifs sur le sous-réseau du dispositif :

1. Choisissez Manage (Gérer) > Discover Devices - LX Subnet (Détecter les dispositifs - Sous-réseau de LX). La page Discover Devices - LX Subnet (Détecter les dispositifs - Sous-réseau de LX) apparaît.
2. Cliquez sur Refresh (Actualiser). La liste des dispositifs du sous-réseau KX est actualisée.

Pour ajouter des dispositifs à votre liste de favoris :

1. Cochez la case située en regard du nom du dispositif/de l'adresse IP.
2. Cliquez sur Add (Ajouter).

Pour accéder à un dispositif détecté :

- Cliquez sur le nom du dispositif ou sur son adresse IP. Un nouveau navigateur s'ouvre pour le dispositif en question.

Ajout, suppression et modification des favoris

Pour ajouter un dispositif dans votre liste de favoris :

1. Sélectionnez Manage Favorites (Gérer les favoris) > Add New Device to Favorites (Ajouter un nouveau dispositif aux favoris). La page Add New Favorite (Ajouter un nouveau favori) apparaît.
2. Saisissez une description significative.
3. Entrez l'adresse IP ou le nom d'hôte du dispositif.
4. Modifiez le port de détection (le cas échéant).
5. Sélectionnez le type de produit.
6. Cliquez sur OK. Le dispositif est ajouté à votre liste de favoris.

Pour modifier un favori :

1. Dans la page Favorites List (Liste des favoris), cochez la case située en regard du dispositif LX approprié.
2. Cliquez sur Modifier. La page Edit (Modifier) apparaît.
3. Mettez à jour les champs, le cas échéant :
   - Description
   - IP Address/Host Name (Adresse IP/Nom d'hôte) - Entrez l'adresse IP du dispositif LX.
   - Port (si nécessaire)
   - Product Type (Type de produit).
4. Cliquez sur OK.

Pour supprimer un favori :

Important : soyez prudent lorsque vous supprimez des favoris. Vous êtes invité à en confirmer la suppression.

1. Cochez la case en regard du dispositif LX approprié.
2. Cliquez sur Delete (Supprimer). Le favori est supprimé de la liste.

Se déconnecter

Pour quitter LX :

- Cliquez sur Logout (Se déconnecter) dans le coin supérieur droit de la page.

Remarque : la déconnexion ferme également toutes les sessions ouvertes de Virtual KVM Client, ainsi que les sessions client série.

Configuration du serveur proxy à utiliser avec MPC, VKC et AKC

Lorsque l'utilisation d'un serveur proxy est requise, un proxy SOCKS doit également être fourni et configuré sur le PC client distant.

Remarque : si le serveur proxy installé n'accepte que le protocole proxy HTTP, vous ne pourrez pas vous connecter.

Pour configurer le proxy SOCKS :

1. Sur le client, sélectionnez Panneau de configuration > Options Internet.

a. Sur l'onglet Connexions, cliquez sur Paramètres réseau. La boîte de dialogue Paramètres du réseau local s'ouvre.

b. Cochez Utiliser un serveur proxy pour votre réseau local.

c. Cliquez sur Avancé. La boîte de dialogue Paramètres du proxy s'ouvre.

d. Configurez les serveurs proxy pour tous les protocoles. IMPORTANT : ne cochez pas la case Utiliser le même serveur proxy pour tous les protocoles.

Remarque : le port par défaut d'un proxy SOCKS (1080) est différent de celui du proxy HTTP (3128).

---

2. Cliquez sur OK dans chaque boîte de dialogue pour appliquer les paramètres.

3. Configurez ensuite les proxys des applets Java™ en sélectionnant Panneau de configuration > Java.

e. Sur l'onglet Général, cliquez sur Paramètres réseau. La boîte de dialogue Paramètres réseau s'ouvre.

f. Sélectionnez Utiliser un serveur proxy.

g. Cliquez sur Avancé. La boîte de dialogue Paramètres réseau avancés s'ouvre.

h. Configurez les serveurs proxy pour tous les protocoles. IMPORTANT : ne cochez pas la case Utiliser le même serveur proxy pour tous les protocoles.

Remarque : le port par défaut d'un proxy SOCKS (1080) est différent de celui du proxy HTTP (3128).

---

4. Si vous utilisez MPC autonome, vous devez également effectuer les opérations suivantes :

i. Ouvrez le fichier start.bat du répertoire MPC à l'aide d'un éditeur de texte.

j. Insérez les paramètres suivants à la ligne de commande. Ajoutez-les avant "-classpath": -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

Les paramètres doivent ressembler à ce qui suit :

start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70 -XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true -DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080 -classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar com.raritan.rrc.ui.RRCApplication %1

Virtual KVM Client (VKC) et Active KVM Client (AKC)

Virtual KVM Client (VKC) et Active KVM Client (AKC) sont des interfaces permettant d'accéder à des cibles distantes. AKC et VKC offrent des fonctions similaires à l'exception des suivantes :

- Configuration système minimale requise
- Systèmes d'exploitation et navigateurs pris en charge
- Les macros de clavier créées dans AKC ne peuvent pas être utilisées dans VKC.
- Configuration de l'accès direct aux ports (reportez-vous à **Activation d'un accès direct aux ports via URL** (à la page 142))
- Configuration de la validation de la certification du serveur AKC (reportez-vous à **Conditions requises pour l'utilisation d'AKC**)

A propos de Virtual KVM Client

Chaque fois que vous accédez à un serveur cible à l'aide de la console distante, une fenêtre Virtual KVM Client (VKC) s'ouvre. A chaque serveur cible connecté correspond une fenêtre Virtual KVM Client. Ces fenêtres sont accessibles via la barre de tâches Windows®.

Remarque : certaines fonctions, telles que les paramètres de lancement client et les cartes à puce, ne sont pas prises en charge par LX et donc, par AKC ou VKC lorsqu'elles sont utilisées conjointement à LX.

Remarque : KX II-101-V2 ne prend en charge qu'une connexion à une cible à la fois.

Elles peuvent être réduites, agrandies et déplacées sur le bureau de votre ordinateur.

Remarque : le rafraîchissement de votre navigateur HTML entraîne la fermeture de la connexion de Virtual KVM Client ; faites donc attention.

Remarque : si vous utilisez Firefox 3.0.3, vous pouvez rencontrer des problèmes de lancement de l'application. Si cela se produit, effacez la mémoire cache du navigateur et lancez l'application à nouveau.

A propos d'Active KVM Client

AKC est basé sur la technologie Microsoft Windows .NET et permet d'exécuter le client dans des environnements Windows sans utiliser Java Runtime Environment (JRE), qui est obligatoire pour exécuter Virtual KVM Client (VKC) et Multi-Platform Client (MPC) de Raritan.

Remarque : certaines fonctions, telles que les paramètres de lancement client et les cartes à puce, ne sont pas prises en charge par LX et donc, par AKC ou VKC lorsqu'elles sont utilisées conjointement à LX.

Systèmes d'exploitation, .NET Framework et navigateurs pris en charge par AKC

.NET Framework

AKC requiert la version 3.5 de Windows .NET®, et fonctionne si les versions 3.5 et 4.0 sont installées, mais non avec la version 4.0 seule.

Systèmes d'exploitation

Lorsqu'il est lancé depuis Internet Explorer®, AKC permet d'atteindre les serveurs cible via KX II 2.2 (et supérieur) et LX 2.4.5 (et supérieur). AKC est compatible avec les plates-formes suivantes exécutant .NET Framework 3.5 :

- système d'exploitation Windows XP®
- système d'exploitation Windows Vista® (jusqu'à 64 bits)
- système d'exploitation Windows 7® (jusqu'à 64 bits)

L'exécution d'AKC requiert .NET. S'il n'est pas installé ou si la version installée n'est pas prise en charge, vous recevrez un message vous demandant de vérifier la version de .NET.

Navigateur

- Internet Explorer 6 ou supérieur

Si vous tentez d'ouvrir AKC à partir d'un navigateur autre qu'IE 6 ou supérieur, vous recevrez un message d'erreur vous demandant de vérifier votre navigateur et d'utiliser Internet Explorer.

Conditions requises pour l'utilisation d'AKC

Pour utiliser AKC :

- Vérifiez que les cookies de l'adresse IP du dispositif auquel vous accédez ne sont pas bloqués.
- Les utilisateurs de serveurs Windows Vista, Windows 7 et Windows 2008 doivent s'assurer que l'adresse IP du dispositif auquel ils accèdent est incluse dans la zone Sites approuvés de leur navigateur et que le mode protégé n'est pas activé lors de l'accès au dispositif.

Activer la validation du certificat du serveur de téléchargement AKC

Si l'administrateur du dispositif a activé l'option Enable AKC Download Server Certificate Validation (Activer la validation du certificat du serveur de téléchargement AKC) :

- Les administrateurs doivent téléverser un certificat valide sur le dispositif ou générer un certificat auto-signé sur celui-ci. Le certificat doit désigner un hôte valide.
- Chaque utilisateur doit ajouter le certificat AC (ou une copie du certificat auto-signé) dans la liste Autorités de certification racines de confiance de leur navigateur.

Barre d'outils

Bouton	Nom du bouton	Description
	Propriétés de connexion	Ouvre la boîte de dialogue Modify Connection Properties (Modifier les propriétés de connexion) à partir de laquelle vous pouvez manuellement définir les options de bande passante (telles que la vitesse de connexion, le nombre de couleurs, etc.).
	Video Settings (Paramètres vidéo)	Ouvre la boîte de dialogue Video Settings (Paramètres vidéo) qui permet de définir manuellement les paramètres de conversion des signaux vidéo.
	Color Calibration (Calibrage des couleurs)	Ajuste les paramètres de couleur de manière à réduire le bruit de couleur superflu. Revient à choisir Video > Color Calibrate (Calibrage des couleurs). *Remarque : non disponible dans KX II-101-V2.*
	Target Screenshot (Capture	Cliquez pour effectuer une capture d'écran du serveur cible et l'enregistrer dans un fichier de votre choix.

Bouton	Nom du bouton	Description
	d'écran de la cible)	
	Audio	Ouvre une boîte de dialogue qui permet d'effectuer une sélection dans une liste de dispositifs audio reliés à un PC client. Une fois les dispositifs audio connectés à la cible, sélectionnez cette option pour les déconnecter. *Remarque : Cette fonction est disponible avec KX II 2.4.0 (et supérieur).* *Remarque : cette fonction n'est pas prise en charge par LX.*
	Synchronize Mouse (Synchroniser la souris)	En mode souris double, force le réalignement du pointeur de la souris du serveur cible sur le pointeur de la souris. *Remarque : non disponible dans KX II-101-V2.*
	Refresh Screen (Actualiser l'écran)	Force le rafraîchissement de l'écran vidéo.
	Auto-sense Video Settings (Détection automatique des paramètres vidéo)	Force le rafraîchissement des paramètres vidéo (résolution, taux de rafraîchissement).
	Smart Card (Carte à puce)	Ouvre une boîte de dialogue qui permet d'effectuer une sélection dans une liste de lecteurs de cartes à puce reliés à un PC client. *Remarque : Cette fonction est disponible uniquement sur KSX II 2.3.0 (et supérieur) et sur KX II 2.1.10 (et supérieur).* *Remarque : cette fonction n'est pas prise en charge par LX.*

Bouton	Nom du bouton	Description
	Send Ctrl+Alt+Del (Envoyer Ctrl+Alt+Suppr)	Envoie la combinaison de touches de raccourci Ctrl+Alt+Suppr au serveur cible.
	Single Cursor Mode (Mode curseur simple)	Démarre le mode curseur simple par lequel le pointeur de souris locale n'apparaît plus à l'écran. Pour quitter ce mode, appuyez sur Ctrl+Alt+O. *Remarque : non disponible dans KX II-101-V2.*
	Mode Full Screen (Mode Plein écran)	Agrandit la zone de l'écran afin d'afficher le Bureau du serveur cible.
	Scaling (Mise à l'échelle)	Augmente ou réduit la taille de la vidéo cible de manière à afficher la totalité du contenu de la fenêtre du serveur cible sans l'aide de la barre de défilement.

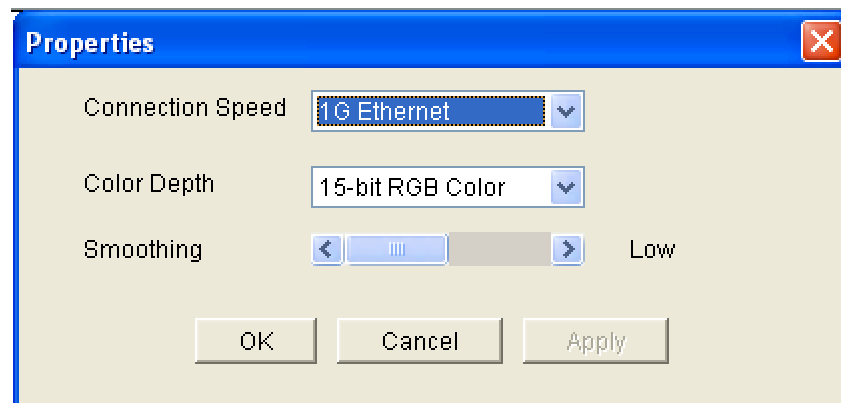
Connection Properties (Propriétés de la connexion)

Les algorithmes de compression vidéo dynamique maintiennent le caractère convivial des consoles KVM avec différents types de bande passante. Les dispositifs optimisent la sortie KVM pour l'utilisation dans un réseau local, mais également pour l'utilisation dans un réseau étendu. Ces dispositifs peuvent également contrôler le nombre de couleurs et limiter la sortie vidéo permettant ainsi un équilibre optimal entre qualité vidéo et réactivité du système pour n'importe quelle bande passante.

Les paramètres de la boîte de dialogue Properties (Propriétés) peuvent être optimisés pour répondre à vos critères spécifiques selon les différents environnements d'exploitation. Les propriétés de connexion sont enregistrées pour les connexions suivantes sur des dispositifs de deuxième génération une fois paramétrées et enregistrées.

Pour définir les propriétés de connexion :

1. Choisissez Connection (Connexion) > Properties (Propriétés) ou cliquez sur le bouton Connection Properties (Propriétés de connexion) de la barre d'outils. La boîte de dialogue Properties (Propriétés) s'ouvre.



Remarque : KX II-101 ne prend pas en charge Ethernet 1G.

2. Sélectionnez une valeur dans la liste déroulante Connection Speed (Vitesse de connexion). Le dispositif peut détecter automatiquement la basse passante disponible et ne pas en restreindre l'utilisation. Cependant, vous pouvez également en régler l'utilisation en fonction des limitations de bande passante.
   - Auto
   - Ethernet 1 G
   - Ethernet 100 Mo
   - Ethernet 10 Mo

- 1,5 Mo (MAX DSL/T1)
- 1 Mo (DSL/T1 rapide)
- 512 Ko (DSL/T1 moyen)
- 384 Ko (DSL/T1 lent)
- 256 Ko (Câble)
- 128 Ko (RNIS double)
- 56 Ko (Modem ISP)
- 33 Ko (Modem rapide)
- 24 Ko (Modem lent)

Notez que ces paramètres représentent des valeurs optimales dans des conditions spécifiques plutôt que le débit exact. Le client et le serveur s'efforcent de transmettre les données vidéo aussi rapidement que possible sur le réseau quels que soient la vitesse réseau et le paramètre d'encodage. Le système sera cependant plus réactif si les paramètres coïncident avec l'environnement réel.

3. Sélectionnez une valeur dans la liste déroulante Color Depth (Nombre de couleurs). Le dispositif peut adapter de manière dynamique le nombre de couleurs transmis aux utilisateurs distants afin d'optimiser la convivialité pour toutes les bandes passantes.

- Couleurs RVB 15 bits
- Couleurs RVB 8 bits
- Couleurs 4 bits
- Gris 4 bits
- Gris 3 bits
- Gris 2 bits
- Noir et blanc

Important : pour la plupart des tâches d'administration (surveillance de serveur, reconfiguration, etc.), l'ensemble du spectre de couleurs 24 bits ou 32 bits disponible avec la plupart des cartes graphiques modernes n'est pas nécessaire. Les tentatives de transmission d'un nombre de couleurs aussi élevé entraîne une perte de bande passante du réseau.

4. Utilisez le curseur pour sélectionner le niveau de lissage souhaité (mode couleurs 15 bits uniquement). Le niveau de lissage détermine le degré de fusion des zones de l'écran aux variations de couleurs faibles en une couleur unique et uniforme. Le lissage améliore l'apparence des vidéos cible en réduisant les bruits vidéo affichés.
5. Cliquez sur OK pour conserver ces propriétés.

Informations sur la connexion

Pour obtenir des informations sur votre connexion à Virtual KVM Client :

- Sélectionnez Connection (Connexion) > Info... La fenêtre d'informations sur la connexion s'affiche alors.

Les informations suivantes relatives à la connexion en cours s’affichent :

- Device Name : nom du dispositif.
- IP Address : adresse IP du dispositif.
- Port : port TCP/IP de communication KVM utilisé pour l'accès au dispositif cible.
- Data In/Second : débit des données en entrée.
- Data Out/Second : débit des données en sortie.
- Connect Time : durée du temps de connexion.
- FPS : nombre d'images par seconde transmises pour la vidéo.
- Horizontal Resolution : résolution d'écran horizontale.
- Vertical Resolution : résolution d'écran verticale.
- Refresh Rate : fréquence à laquelle l'écran est actualisé.
- Protocol Version : version du protocole RFB.

Pour copier ces informations :

- Cliquez sur Copy to Clipboard (Copier dans Presse-papiers). Ces informations peuvent maintenant être copiées dans le programme de votre choix.

Options de clavier

Macros de clavier

Les macros de clavier garantissent l'envoi des frappes destinées au serveur cible et leur interprétation par le serveur cible uniquement. Sinon, elles risqueraient d'être interprétées par l'ordinateur sur lequel est exécuté Virtual KVM Client (votre PC client).

Les macros sont stockées sur le PC client et sont spécifiques au PC. Aussi, si vous utilisez un autre PC, vous ne voyez pas vos macros. Par ailleurs, si un autre utilisateur utilise votre PC et se connecte sous un nom différent, il verra vos macros puisqu'elles font partie intégrante de l'ordinateur.

Les macros de clavier créées dans Virtual KVM Client sont disponibles dans MPC et inversement. Toutefois, les macros de clavier créées dans Active KVM Client (AKC) ne peuvent pas être utilisées dans VKC ou MPC, et inversement.

Remarque : KX II-101 ne prend pas en charge AKC.

Importation/exportation de macros de clavier

Les macros exportées d'Active KVM Client (AKC) ne peuvent pas être importées dans Multi-Platform Client (MPC) ou Virtual KVM Client (VKC). Les macros exportées de MPC ou VKC ne peuvent pas être importées dans AKC.

Remarque : KX II-101 ne prend pas en charge AKC.

Pour importer des macros :

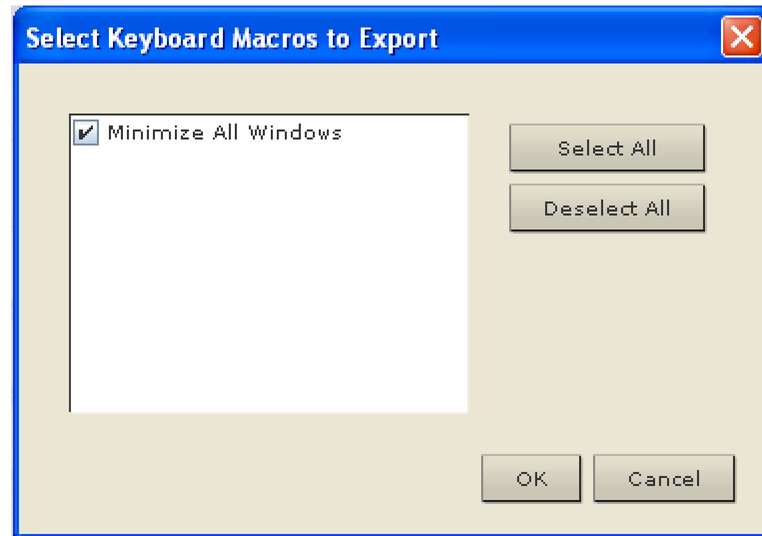
1. Choisissez Keyboard > Import Keyboard Macros (Clavier > Importer des macros de clavier) pour ouvrir la boîte de dialogue Import Macros (Importation de macros). Accédez à l'emplacement du dossier du fichier de macro.
2. Cliquez sur le fichier de macro et cliquez sur Ouvrir pour importer la macro.
   a. Si le fichier comporte trop de macros, un message d'erreur s'affiche et l'importation s'interrompt lorsque vous cliquez sur OK.
   b. Si l'importation échoue, une boîte de dialogue d'erreur apparaît contenant un message indiquant le motif de l'échec. Sélectionnez OK pour continuer l'importation en évitant les macros ne pouvant pas être traitées.
3. Sélectionnez les macros à importer en cochant la case correspondante ou en utilisant les options Select All (Tout sélectionner) ou Deselect All (Tout désélectionner).

4. Cliquez sur OK pour démarrer l'importation.
   a. Si une macro en double est détectée, la boîte de dialogue Import Macros (Importer des macros) apparaît. Effectuez une des opérations suivantes :
      - Cliquez sur Yes (Oui) pour remplacer la macro existante par la version importée.
      - Cliquez sur Yes to All (Oui pour tout) pour remplacer la macro sélectionnée et toutes les autres en double éventuellement détectées.
      - Cliquez sur No (Non) pour conserver la macro d'origine et passer à la suivante.
      - Cliquez sur No to All (Non pour tout) pour conserver la macro d'origine et passer à la suivante. Les autres doubles détectés sont également ignorés.
      - Cliquez sur Cancel (Annuler) pour arrêter l'importation.
      - Vous pouvez également cliquer sur Rename pour renommer la macro et l'importer. La boîte de dialogue Rename Macro (Renommage de la macro) apparaît. Entrez le nouveau nom de la macro dans le champ et cliquez sur OK. La boîte de dialogue se ferme et la procédure continue. Si le nom entré est le double d'une macro, une alerte apparaît et vous devez donner un autre nom à la macro.
   b. Si, au cours de l'importation, le nombre de macros importées autorisé est dépassé, une boîte de dialogue apparaît. Cliquez sur OK pour tenter de poursuivre l'importation des macros ou cliquez sur Cancel (Annuler) pour l'arrêter.

Les macros sont alors importées. Si une macro importée contient un raccourci-clavier existant, celui-ci est éliminé.

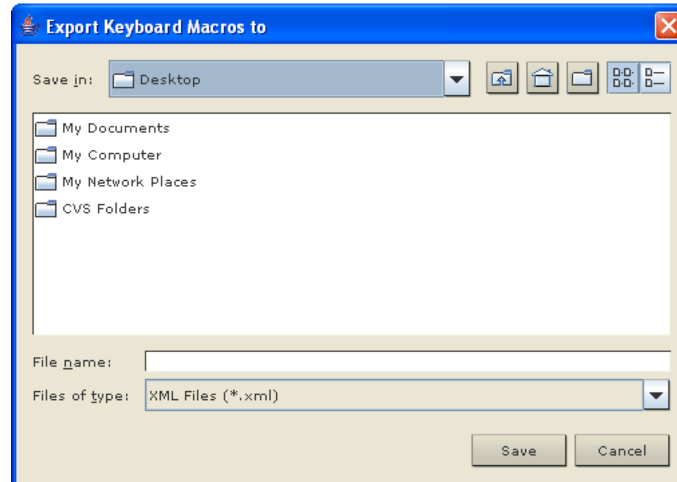
Pour exporter des macros :

1. Choisissez Tools > Export Macros (Outils > Exportation de macros) pour ouvrir la boîte de dialogue Select Keyboard Macros to Export (Sélectionnez les macros de clavier à exporter).



2. Sélectionnez les macros à exporter en cochant la case correspondante ou en utilisant les options Select All (Tout sélectionner) ou Deselect All (Tout désélectionner).
3. Cliquez sur OK. Une boîte de dialogue apparaît permettant de localiser et de sélectionner le fichier de macro. Par défaut, la macro existe sur votre bureau.

4. Sélectionnez le dossier d'enregistrement du fichier de macro, entrez le nom du fichier et cliquez sur Save (Enregistrer). Si la macro existe déjà, vous recevez un message d'alerte. Sélectionnez Yes (Oui) pour écraser la macro existante ou No (Non) pour fermer l'alerte sans écraser la macro.



Définition d'une macro de clavier

Pour créer une macro :

1. Cliquez sur Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Cliquez sur Add (Ajouter). La boîte de dialogue Add Keyboard Macro (Ajouter une macro de clavier) s'affiche.
3. Saisissez un nom dans le champ Keyboard Macro Name (Nom de la macro de clavier). Une fois la macro créée, ce nom apparaît dans le menu Keyboard (Clavier).
4. Dans la liste déroulante Hot-Key Combination (Raccourci-clavier), sélectionnez un raccourci-clavier. Vous pouvez ainsi exécuter la macro à l'aide d'une touche prédéfinie. **Facultatif**
5. Dans la liste déroulante Keys to Press (Touches à enfoncer), sélectionnez chaque touche que vous souhaitez employer afin d'émuler les frappes utilisées pour exécuter la commande. Sélectionnez les touches dans l'ordre où elles doivent être enfoncées. Après chaque sélection, choisissez Add Key (Ajouter la touche). Après avoir été sélectionnée, chaque touche apparaît dans le champ Macro Sequence (Séquence de la macro) et une commande Release Key (Relâcher la touche) est ajoutée automatiquement après chaque sélection.

6. Pour utiliser la fonction Send Text to Target (Envoyer du texte à la cible) dans la macro, cliquez sur le bouton Construct Macro from Text (Construire la macro à partir de texte).
7. Par exemple, créez une macro pour fermer une fenêtre en sélectionnant Ctrl gauche + Echap. Ceci apparaît dans la zone Macro Sequence comme suit :

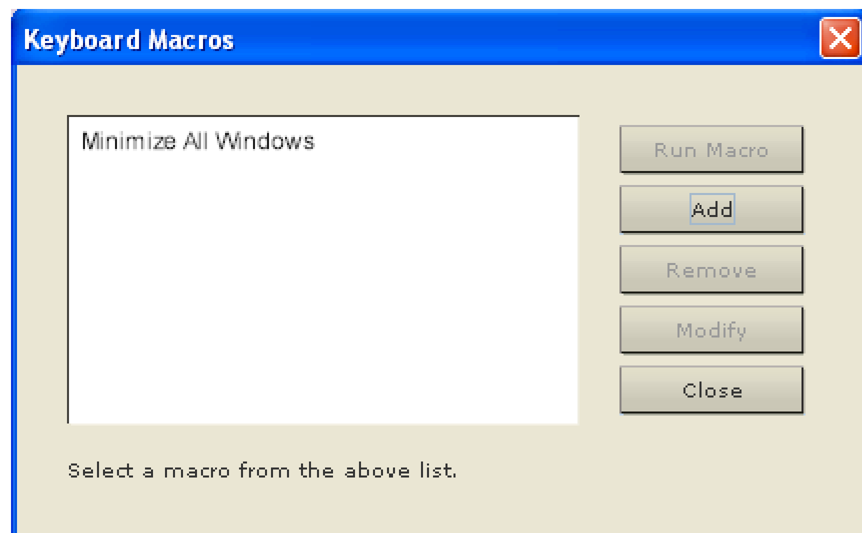
    Press Left Ctrl (Appuyer sur Ctrl gauche)

    Release Left Ctrl (Relâcher Ctrl gauche)

    Press Esc (Appuyer sur Echap)

    Release Esc (Relâcher Echap)

8. Passez en revue le champ Macro Sequence pour vous assurer que la séquence de la macro est définie correctement.
    a. Pour supprimer une étape de la séquence, sélectionnez l'étape et cliquez sur Remove (Supprimer).
    b. Pour modifier l'ordre des étapes dans la séquence, cliquez sur l'étape, puis sur les flèches haut ou bas pour établir l'ordre souhaité.
9. Cliquez sur OK pour enregistrer la macro. Cliquez sur Clear (Effacer) pour effacer le contenu des champs et recommencer. Lorsque vous cliquez sur OK, la fenêtre Keyboard Macros (Macros de clavier) s'affiche et présente la nouvelle macro de clavier.
10. Cliquez sur Close (Fermer) dans la boîte de dialogue Keyboard Macros (Macros de clavier). La macro apparaît maintenant dans le menu Keyboard (Clavier) de l'application. Sélectionnez la nouvelle macro dans le menu pour l'exécuter ou utilisez les touches que vous lui avez affectées.



Lancement d'une macro de clavier

Une fois que vous avez créé une macro de clavier, exécutez-la à l'aide de la macro de clavier que vous lui avez affectée ou en la choisissant dans le menu Keyboard (Clavier).

Exécution d'une macro à partir de la barre de menus

Lorsque vous créez une macro, elle s'affiche dans le menu Keyboard (Clavier). Exécutez la macro du clavier en cliquant sur son nom dans le menu Keyboard (Clavier).

Exécution d'une macro avec une combinaison de touches

Si vous avez attribué une combinaison de touches à une macro lors de sa création, vous pouvez exécuter la macro en appuyant sur les touches correspondantes. Par exemple, appuyez simultanément sur les touches Ctrl+Alt+0 pour réduire toutes les fenêtres sur un serveur cible Windows.

Modification et suppression des macros de clavier

Pour modifier une macro :

1. Choisissez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Choisissez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur Modify (Modifier). La fenêtre d'ajout/de modification de la macro apparaît.
4. Effectuez vos modifications.
5. Cliquez sur OK.

Pour supprimer une macro :

1. Choisissez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Choisissez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur Remove (Supprimer). La macro est supprimée.

Macro Ctrl+Alt+Suppr

En raison de son utilisation fréquente, une macro Ctrl+Alt+Suppr est préprogrammée. Lorsque vous cliquez sur le bouton Ctrl+Alt+Suppr de la barre d'outils, cette séquence de touches est envoyée au serveur ou au commutateur KVM auquel vous êtes actuellement connecté.

En revanche, si vous appuyiez physiquement sur les touches Ctrl+Alt+Suppr, la commande serait d'abord interceptée par votre propre ordinateur en raison de la structure du système d'exploitation Windows, au lieu d'être envoyée au serveur cible comme prévu.

Paramétrage des options clavier/souris CIM

Pour accéder au menu de configuration de DCIM-USBG2 :

1. Mettez en surbrillance à l'aide de la souris une fenêtre telle que Notepad (système d'exploitation Windows®) ou son équivalent.
2. Sélectionnez les options Set CIM Keyboard/Mouse options (Définir les options clavier/souris CIM). Ceci correspond à l'envoi de touche Ctrl gauche et Verr Num à la cible. Les options du menu de paramètres CIM sont alors affichées.
3. Définissez la langue et les paramètres de souris.
4. Quittez le menu pour retourner à la fonctionnalité CIM normale.

Propriétés vidéo

Actualisation de l'écran

La commande Refresh Screen (Actualiser l'écran) force le rafraîchissement de l'écran vidéo. Les paramètres vidéo peuvent être actualisés automatiquement de plusieurs manières :

- La commande Refresh Screen (Actualiser l'écran) force le rafraîchissement de l'écran vidéo.
- La commande Auto-sense Video Settings (Détection automatique des paramètres vidéo) permet de détecter automatiquement les paramètres vidéo du serveur cible.
- La commande Calibrate Color (Calibrer les couleurs) permet de procéder au calibrage de la vidéo afin d'optimiser les couleurs affichées.

Vous pouvez également régler les paramètres manuellement à l'aide de la commande Video Settings (Paramètres vidéo).

Pour actualiser les paramètres vidéo, effectuez l'une des opérations suivantes :

- Choisissez Video > Refresh Screen (Actualiser l'écran) ou cliquez sur le bouton Refresh Screen de la barre d'outils.

Détection automatique des paramètres vidéo

La commande Auto-sense Video Settings force une nouvelle détection des paramètres vidéo (résolution, taux de rafraîchissement) et redessine l'écran vidéo.

Pour détecter automatiquement les paramètres vidéo :

- Choisissez Video > Auto-sense Video Settings (Détection automatique des paramètres vidéo) ou cliquez sur le bouton Auto-Sense Video Settings de la barre d'outils. Un message s'affiche pour indiquer que le réglage automatique est en cours.

Calibrage de la couleur

Utilisez la commande Calibrate Color pour optimiser les niveaux de couleur (teinte, luminosité, saturation) des images vidéo transmises. Les paramètres couleur concernent le serveur cible.

Remarque : la commande Calibrate Color (Calibrer les couleurs) s'applique à la connexion en cours uniquement.

Remarque : KX II-101 ne prend pas en charge le calibrage des couleurs.

Pour calibrer la couleur :

- Choisissez Video > Calibrate Color (Calibrer les couleurs) ou cliquez sur le bouton Calibrate Color de la barre d'outils. Le calibrage des couleurs de l'écran du dispositif cible est mis à jour.

Ajustement des paramètres vidéo

Utilisez la commande Video Settings (Paramètres vidéo) pour ajuster manuellement les paramètres vidéo.

Pour modifier les paramètres vidéo :

1. Choisissez Video > Video Settings ou cliquez sur le bouton Video Settings de la barre d'outils pour ouvrir la boîte de dialogue du même nom.
2. Définissez les paramètres ci-après, le cas échéant. Les effets sont visibles dès que vous définissez les paramètres :
   a. Noise Filter (Filtre antiparasite)

      Le dispositif ProductName peut supprimer les interférences électriques de la sortie vidéo des cartes graphiques. Cette fonction optimise la qualité des images et réduit la bande passante. Les paramètres plus élevés transmettent des pixels de variante uniquement s'il existe une importante variation de couleurs par rapport aux pixels voisins. Néanmoins, si vous définissez un seuil trop élevé, des modifications souhaitées au niveau de l'écran peuvent être filtrées de manière non intentionnelle.
      Un seuil plus bas permet de transmettre le plus de changements de pixels. Si ce seuil est défini de manière trop faible, l'utilisation de la bande passante risque d'être plus importante.

   b. PLL Settings (Paramètres PPL)

Clock (Horloge) : contrôle la vitesse d'affichage des pixels vidéo sur l'écran vidéo. Les modifications apportées aux paramètres d'horloge entraînent l'étirement ou la réduction de l'image vidéo sur le plan horizontal. Nous vous recommandons d'utiliser des nombres impairs. Dans la majorité des cas, ce paramètre ne doit pas être modifié car la détection automatique est en général très précise.

Phase : les valeurs de phase sont comprises entre 0 et 31 et s'affichent en boucle. Arrêtez-vous à la valeur de phase qui produit la meilleure image vidéo pour le serveur cible actif.

c. Brightness : utilisez cette option pour ajuster la luminosité de l'écran du serveur cible.

d. Brightness Red : contrôle la luminosité de l'écran du serveur cible pour le signal rouge.

e. Brightness Green : contrôle la luminosité du signal vert.

f. Brightness Blue : contrôle la luminosité du signal bleu.

g. Contrast Red : contrôle le contraste du signal rouge.

h. Contrast Green : contrôle le signal vert.

i. Contrast Blue : contrôle le signal bleu.

Si l'image vidéo semble très floue ou que sa mise au point ne semble pas correcte, les paramètres d'horloge et de phase peuvent être ajustés jusqu'à ce qu'une image de meilleure qualité s'affiche sur le serveur cible actif.

Avertissement : soyez prudent lorsque vous modifiez les paramètres Clock and Phase (Horloge et phase) ; en effet ces modifications peuvent entraîner des pertes ou des distorsions vidéo et vous risquez de ne plus pouvoir rétablir l'état précédent. Contactez l'assistance technique Raritan avant d'effectuer tout changement.

---

j. Horizontal Offset (Décalage horizontal) : contrôle le positionnement horizontal de l'affichage du serveur cible sur votre écran.

k. Vertical Offset (Décalage vertical) : contrôle le positionnement vertical de l'affichage du serveur cible sur votre écran.

3. Sélectionnez Automatic Color Calibration (Calibrage automatique des couleurs) pour activer cette fonction.

4. Sélectionnez le mode de détection vidéo :

   - Best possible video mode (Mode vidéo optimal) :

   le dispositif effectue la totalité du processus de détection automatique lorsque vous changez de cibles ou de résolutions cible. La sélection de cette option calibre la vidéo pour obtenir la qualité d'image optimale.

- Quick sense video mode (Détection rapide du mode vidéo) :

  avec cette option, le dispositif utilise la détection rapide automatique du mode vidéo pour afficher au plus vite le signal vidéo de la cible. Cette option est particulièrement utile lors de la saisie de la configuration BIOS d'un serveur cible immédiatement après un redémarrage.

5. Cliquez sur OK pour appliquer les paramètres et fermer la boîte de dialogue. Cliquez sur Apply pour appliquer les paramètres sans fermer la boîte de dialogue.

Remarque : certains écrans d'arrière-plan Sun, tels que les écrans à bord très sombres, risquent de ne pas se centrer de façon précise sur certains serveurs Sun. Utilisez un arrière-plan différent ou une icône de couleur plus claire dans le coin supérieur gauche de l'écran.

Video Settings

Noise Filter

Noise Filter: 2 0 7

PLL Settings

Clock: 1,344 1026 1844

Phase: 26 0 31

Color Settings

Brightness Red: 44 0 127

Brightness Green: 64 0 127

Brightness Blue: 43 0 127

Contrast Red: 214 0 255

Contrast Green: 219 0 255

Contrast Blue: 219 0 255

Horizontal Offset: 282 0 318

Vertical Offset: 35 0 37

Automatic Color Calibration

Video Sensing

Best possible video mode

Quick sense video mode

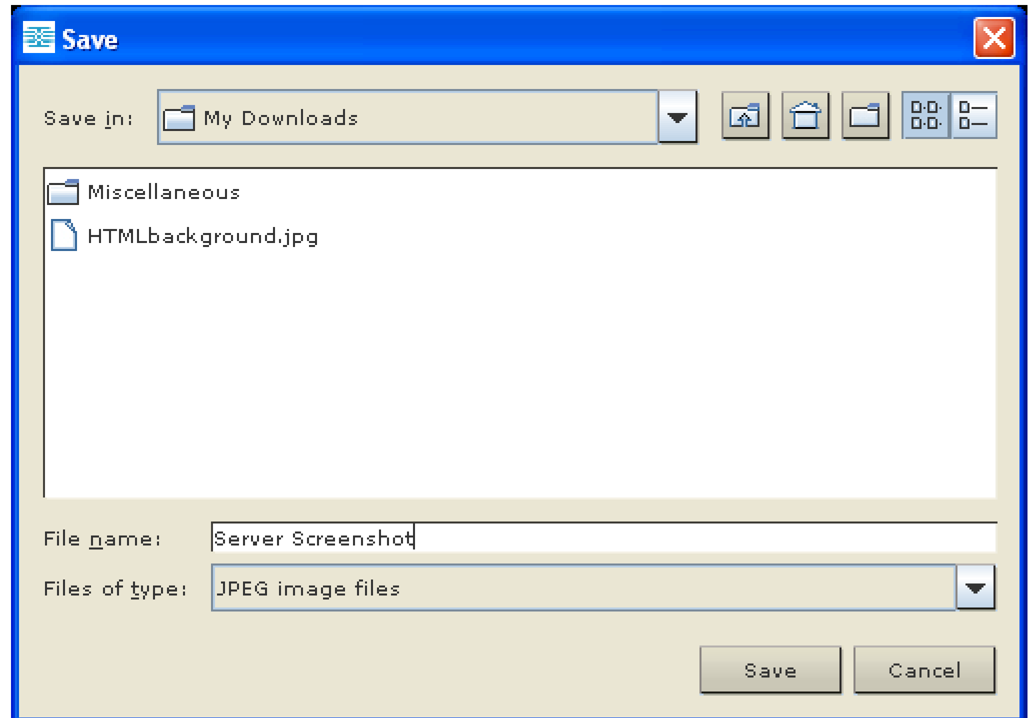
OK Cancel Apply

Utilisation de la commande Screenshot from Target

La commande serveur Screenshot from Target (Capture d'écran de la cible) vous permet d'effectuer une capture d'écran du serveur cible. Au besoin, enregistrez cette capture d'écran à un emplacement de votre choix dans un fichier bitmap, JPEG ou PNG.

Pour effectuer une capture d'écran du serveur cible :

1. Sélectionnez Video (Vidéo) > Screenshot from Target (Capture d'écran de la cible) ou cliquez sur le bouton dans la barre d'outils.
2. Dans la boîte de dialogue Save (Enregistrer), choisissez l'emplacement de sauvegarde du fichier, nommez le fichier et sélectionnez un format dans la liste déroulante Type de fichiers.
3. Cliquez sur Save (Enregistrer) pour enregistrer la capture.



Modification du taux de rafraîchissement maximum

Si la carte vidéo dont vous disposez utilise un logiciel personnalisé et que vous accédez à la cible par l'intermédiaire de MPC ou de VKC, il vous faudra sans doute modifier le taux maximum de rafraîchissement de l'écran pour que celui-ci prenne effet sur la cible.

▶ **Pour régler le taux de rafraîchissement de l'écran :**

1. Sous Windows®, sélectionnez Propriétés d'affichage < Paramètres < Avancé pour ouvrir la boîte de dialogue Plug-and-Play.
2. Cliquez sur l'onglet Moniteur.
3. Définissez la fréquence de rafraîchissement du moniteur.
4. Cliquez sur OK, puis à nouveau sur OK pour appliquer le paramètre.

Options de souris

Lors de la gestion d'un serveur cible, la console distante affiche deux curseurs de souris : un curseur correspond à votre poste de travail client et l'autre, au serveur cible.

Vous avez la possibilité d'opérer soit en mode de souris simple, soit en mode de souris double. En mode souris double, et à condition que l'option soit correctement configurée, les curseurs s'alignent.

En présence de deux curseurs de souris, le dispositif propose plusieurs modes de souris :

- Absolute (Absolu) (Synchronisation de la souris)
- Intelligent (Mode de souris)
- Standard (Mode de souris)

Synchronisation des pointeurs de souris

Lorsque vous affichez à distance un serveur cible utilisant une souris, deux curseurs de souris apparaissent : un curseur correspond à votre poste de travail client distant et l'autre au serveur cible. Lorsque le pointeur de votre souris se trouve dans la zone de la fenêtre du serveur cible de Virtual KVM Client, les mouvements et les clics de souris sont directement transmis au serveur cible connecté. Lorsqu'il est en mouvement, le pointeur de la souris du client est légèrement en avance sur celui de la souris de la cible en raison des paramètres d'accélération de souris.

Avec des connexions de réseau local rapides, vous pouvez désactiver le pointeur de la souris de Virtual KVM Client et afficher uniquement le pointeur de la souris du serveur cible. Vous pouvez basculer entre ces deux modes souris (simple et double).

Conseils de synchronisation de la souris

Veillez à suivre ces étapes lorsque vous configurez la synchronisation des souris :

1. Vérifiez que la résolution vidéo et le taux de rafraîchissement sélectionnés sont pris en charge par le dispositif. La boîte de dialogue Virtual KVM Client Connection Info (Informations sur la connexion de Virtual KVM Client) affiche les valeurs réellement observées par le dispositif.
2. Pour les dispositifs KX II et LX, assurez-vous que la longueur de câble se trouve dans les limites spécifiées pour la résolution vidéo sélectionnée.
3. Vérifiez que la souris et la vidéo ont été configurées correctement au cours de l'installation.
4. Forcez la détection automatique en cliquant sur le bouton de détection automatique de Virtual KVM Client.
5. Si cela n'améliore pas la synchronisation de la souris (pour des serveurs cible KVM Linux, UNIX et Solaris) :
   a. Ouvrez une fenêtre de terminal.
   b. Entrez la commande `xset mouse 1 1`.
   c. Fermez la fenêtre de terminal.
6. Cliquez sur le bouton de synchronisation de la souris de Virtual KVM Client .

Remarques supplémentaires sur le mode souris intelligente

- Aucune icône ou application ne doit se trouver dans la partie supérieure gauche de l'écran dans la mesure où la routine de synchronisation a lieu à cet emplacement.
- N'utilisez pas de souris animée.
- Désactivez le bureau actif sur les serveurs cible KVM.

Synchronize Mouse (Synchroniser la souris)

En mode souris double, la commande Synchronize Mouse (Synchroniser la souris) force un nouvel alignement du pointeur de la souris du serveur cible avec le pointeur de la souris de Virtual KVM Client.

Pour synchroniser la souris, effectuez l'une des opérations suivantes :

- Choisissez Mouse (Souris) > Synchronize Mouse (Synchroniser la souris) ou cliquez sur le bouton Synchronize Mouse de la barre d'outils.

Remarque : Cette option est disponible uniquement pour les modes de souris standard et intelligente.

Mode souris standard

Le mode souris standard utilise un algorithme de synchronisation de souris standard reprenant les positions de souris relatives. Le mode souris standard requiert la désactivation de l'accélération de la souris et que les autres paramètres de souris soient configurés correctement afin que la souris du client et celle du serveur restent synchronisées.

Pour entrer en mode souris standard :

- Choisissez Mouse (Souris) > Standard.

Mode souris intelligente

En mode souris intelligente, le dispositif peut détecter les paramètres de la souris cible et synchroniser les curseurs de souris en conséquence, permettant une accélération de la souris au niveau de la cible. Le mode de souris intelligente est le mode par défaut des cibles non-VM.

Au cours de la synchronisation, le curseur de souris effectue une « danse » dans le coin supérieur gauche de l'écran et calcule l'accélération. Pour que ce mode fonctionne correctement, certaines conditions doivent être remplies.

▶ **Pour entrer en mode souris intelligente :**

- Sélectionnez Mouse (Souris) > Intelligent (Intelligente).

Conditions de synchronisation d'une souris intelligente

La commande Intelligent Mouse Synchronization (Synchronisation de souris intelligente), disponible dans le menu Mouse (Souris) synchronise automatiquement les curseurs de souris lors des moments d'inactivité. Cependant, pour que cette option fonctionne correctement, les conditions suivantes doivent être remplies :

- Le bureau actif doit être désactivé sur le serveur cible.
- Aucune fenêtre ne doit apparaître dans le coin supérieur gauche de la page cible.
- Le coin supérieur gauche de la page cible ne doit pas comporter d'arrière-plan animé.
- La forme du pointeur de la souris cible doit être normale et non animée.
- La vitesse de déplacement du pointeur de souris du serveur cible ne doit pas être réglée sur une valeur très basse ou très élevée.
- Les propriétés de souris avancées, telles que Enhanced pointer precision (Améliorer la précision du pointeur) ou Snap mouse to default button in dialogs (Déplacer automatiquement le pointeur sur le bouton par défaut dans les boîtes de dialogue) doivent être désactivées.
- Les utilisateurs doivent sélectionner l'option Best Possible Video Mode (Mode vidéo optimal) dans la fenêtre Video Settings (Paramètres vidéo).
- Les bords de l'affichage vidéo du serveur cible doivent être clairement visibles (une bordure noire doit être visible entre le bureau de la cible et la fenêtre de la console KVM distante lorsque vous affichez un bord de l'image vidéo de la cible).

- La fonction de synchronisation de la souris intelligente risque de ne pas fonctionner correctement si vous avez une icône de fichier ou de dossier dans le coin supérieur gauche du bureau. Pour éviter tout problème avec cette fonction, Raritan vous recommande de ne pas avoir d'icônes de fichier ou de dossier dans le coin supérieur gauche de votre bureau.

Après avoir exécuté la fonction de détection automatique des paramètres vidéo, exécutez manuellement la synchronisation de la souris en cliquant sur le bouton Synchronize Mouse (Synchroniser la souris) dans la barre d'outils. Cette recommandation est également valable si la résolution du serveur cible est modifiée, entraînant une désynchronisation des pointeurs de souris.

Si la synchronisation de souris intelligente échoue, la souris reprend son comportement standard.

Notez que les configurations de souris varient selon le système d'exploitation cible. Reportez-vous aux instructions de votre système d'exploitation pour de plus amples informations. Notez également que la synchronisation intelligente de la souris ne fonctionne pas avec les cibles UNIX.

Mode souris absolue

Dans ce mode, des coordonnées absolues sont utilisées pour maintenir la synchronisation des curseurs client et cible, même si l'accélération ou la vitesse de la souris cible est configurée sur une valeur différente. Ce mode est pris en charge sur les serveurs avec ports USB et il s'agit du mode par défaut pour les cibles VM et VM doubles.

▶ Pour entrer en mode souris absolue :

- Sélectionnez Mouse (Souris) > Absolute (Absolue).

Remarque : pour LX, la synchronisation absolue de la souris est disponible uniquement pour les CIM USB pour lesquels le support virtuel est activé (D2CIM-VUSB et D2CIM-DVUSB).

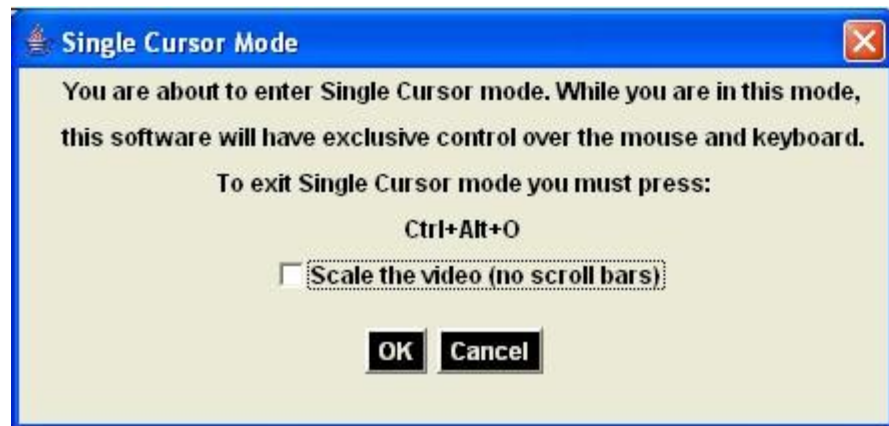
Mode de souris unique

Le mode souris simple utilise uniquement le curseur de la souris du serveur cible ; le pointeur de souris locale n'apparaît plus à l'écran. Si vous êtes en mode souris simple, la commande Synchronize Mouse n'est pas disponible (il n'est pas nécessaire de synchroniser un curseur de souris simple).

Remarque : le mode de souris unique ne fonctionne pas sur des cibles Windows ou Linux lorsque VM est utilisé comme client.

Pour passer en mode souris simple, procédez comme suit :

1. Sélectionnez Mouse (Souris) > Single Mouse Cursor (Curseur de souris simple).
2. Cliquez sur le bouton Single/Double Mouse Cursor (Curseur de souris simple/double) dans la barre d'outils.



Pour quitter le mode souris simple :

- Appuyez sur Ctrl+Alt+O sur le clavier pour quitter le mode souris simple.

Options d'outils

Paramètres généraux

Pour définir les options d'outils :

1. Cliquez sur Tools (Outils) > Options. La boîte de dialogue Options s'affiche.
2. Cochez la case Enable Logging (Activer la journalisation) uniquement si l'assistance technique vous y invite. Cette option permet de créer un fichier journal dans votre répertoire personnel.

3. Sélectionnez le type de clavier (Keyboard Type) dans la liste déroulante (le cas échéant). Les options incluent :
   - US/International (Anglais Etats-Unis/international)
   - Français (France)
   - Allemand (Allemagne)
   - Japonais
   - Royaume-Uni
   - Coréen (Corée)
   - Français (Belgique)
   - Norvégien (Norvège)
   - Portugais (Portugal)
   - Danois (Danemark)
   - Suédois (Suède)
   - Allemand (Suisse)
   - Hongrois (Hongrie)
   - Espagnol (Espagne)
   - Italien (Italie)
   - Slovène
   - Traduction : Français - US
   - Traduction : Français - US International

   dans AKC, le type de clavier provient par défaut du client local, cette option ne s'applique donc pas. En outre, KX II-101 et KX II-101-V2 ne prenant pas en charge le mode de curseur simple, la fonction Exit Single Cursor Mode (Quitter le mode de curseur simple) ne s'applique pas pour ces dispositifs.

4. Configurez les raccourcis-clavier :
   - Exit Full Screen Mode - Hotkey (Quitter le mode Plein écran - Raccourci-clavier). Lorsque vous entrez en mode Plein écran, l'affichage du serveur cible entre en mode Plein écran et acquiert la même résolution que le serveur cible. Il s'agit du raccourci-clavier utilisé pour quitter ce mode.
   - Exit Single Cursor Mode - Hotkey (Quitter le mode de curseur simple - Raccourci-clavier). Lorsque vous entrez en mode de curseur simple, seul le curseur de souris du serveur cible est visible. Il s'agit du raccourci-clavier utilisé pour quitter le mode de curseur simple et rétablir le curseur de souris du client.
   - Disconnect from Target - Hotkey (Se déconnecter de la cible - Raccourci-clavier). Activez ce raccourci-clavier pour permettre aux utilisateurs de se déconnecter rapidement de la cible.

Pour les raccourcis-clavier, l'application n'autorise pas l'affectation de la même combinaison à plusieurs fonctions. Par exemple, si la touche Q est déjà appliquée à la fonction Disconnect from Target (Se déconnecter de la cible), elle ne sera pas disponible pour la fonction Exit Full Screen Mode (Quitter le mode Plein écran). En outre, si un raccourci-clavier est ajouté à l'application en raison d'une mise à niveau et que la valeur par défaut pour la touche est déjà utilisée, la valeur disponible suivante est appliquée à la fonction à la place.

5. Cliquez sur OK.

Restrictions concernant les claviers

Claviers turcs

Si vous utilisez un clavier turc, vous devez vous connecter à un serveur cible via Active KVM Client (AKC). Il n'est pas pris en charge par les autres clients Raritan.

Claviers slovènes

La touche < ne fonctionne pas sur les claviers slovènes à cause d'une restriction JRE.

Configuration des langues étrangères sous Linux

Comme Sun JRE sous Linux a des difficultés à générer les événements clés corrects pour les claviers étrangers configurés à l'aide des préférences du système, Raritan recommande de configurer ces claviers étrangers à l'aide des méthodes utilisées dans le tableau suivant.

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Français	Indicateur de clavier
Allemand	Paramètres système (centre de contrôle)
Japonais	Paramètres système (centre de contrôle)
Anglais britannique	Paramètres système (centre de contrôle)
Coréen	Paramètres système (centre de contrôle)
Belge	Indicateur de clavier
Norvégien	Indicateur de clavier
Danois	Indicateur de clavier
Suédois	Indicateur de clavier
Hongrois	Paramètres système (centre de contrôle)
Espagnol	Paramètres système (centre de contrôle)

Langue/clavier	Méthode de configuration
Italien	Paramètres système (centre de contrôle)
Slovène	Paramètres système (centre de contrôle)
Portugais	Paramètres système (centre de contrôle)

Remarque : l'indicateur de clavier doit être utilisé sur les systèmes Linux utilisant l'environnement de bureau Gnome.

Paramètres de lancement client

Les utilisateurs de LX peuvent configurer des paramètres de lancement client permettant de définir les paramètres d'écran d'une session KVM.

Remarque : Cette fonction est disponible dans MPC, et non dans AKC ou VKC.

Pour configurer les paramètres de lancement client :

1. Cliquez sur Tools (Outils) > Options. La boîte de dialogue Options s'affiche.
2. Cliquez sur l'onglet Client Launch Settings (Paramètres de lancement client).
   - Pour configurer les paramètres de la fenêtre cible :
   a. Sélectionnez Standard - sized to target Resolution (Standard - dimension de la résolution cible) pour ouvrir la fenêtre en utilisant la résolution actuelle de la cible. Si la résolution cible est supérieure à celle du client, la fenêtre cible couvre autant de surface à l'écran que possible et des barres de défilement sont ajoutées (le cas échéant).
   b. Sélectionnez Full Screen (Plein écran) pour ouvrir la fenêtre cible en mode Plein écran.
   - Pour configurer le moniteur de lancement de l'afficheur cible :
   a. Sélectionnez Monitor Client Was Launched from (Moniteur de lancement du client) si vous souhaitez lancer l'afficheur cible à l'aide du même affichage que l'application utilisée sur le client (un navigateur ou une applet Web, par exemple).
   b. Utilisez Select From Detected Monitors (Sélectionner parmi les moniteurs détectés) pour effectuer une sélection dans la liste des moniteurs détectés par l'application. Si un moniteur sélectionné précédemment n'est plus détecté, la mention Currently Selected Monitor Not Detected (Moniteur sélectionné non détecté) apparaît.
   - Pour configurer des paramètres de lancement supplémentaires :

a. Sélectionnez Enable Single Cursor Mode (Activer le mode de curseur simple) pour activer par défaut le mode de curseur simple lors de l'accès au serveur.

b. Sélectionnez Enable Scale Video (Mise à l'échelle de la vidéo) pour mettre à l'échelle automatiquement l'affichage sur le serveur cible lors de l'accès à celui-ci.

c. Sélectionnez Pin Menu Toolbar (Epingler la barre d'outils de menu) si vous souhaitez que la barre d'outils reste visible sur la cible en mode Plein écran. Par défaut, lorsque la cible est en mode Plein écran, le menu n'est visible que lorsque vous faites passer la souris le long du haut de l'écran.

3. Cliquez sur OK.

Paramètres de balayage

LX offre une fonction de balayage des ports qui recherche les cibles sélectionnées et les affiche dans une vue en diaporama, ce qui vous permet de contrôler jusqu'à 32 cibles simultanément. Vous pouvez vous connecter aux cibles ou sélectionner une cible spécifique le cas échéant. Les balayages peuvent inclure des cibles standard, des dispositifs Dominion en niveau et des ports de commutateurs KVM. Reportez-vous à ***Balayage des ports*** (à la page 50). L'onglet Scan Settings (Paramètres de balayage) permet de personnaliser l'intervalle de balayage et les options d'affichage par défaut.

Pour définir les paramètres de balayage :

1. Cliquez sur Tools (Outils) > Options. La boîte de dialogue Options s'affiche.
2. Sélectionnez l'onglet Scan Settings (Paramètres de balayage).
3. Dans le champ Display Interval (10-255 sec) (Intervalle d'affichage (10 à 255 s), indiquez le nombre de secondes pendant lesquelles la cible sélectionnée doit rester affichée au centre de la fenêtre Port Scan (Balayage des ports).
4. Dans le champ Interval Between Ports (10 - 255 sec) (Intervalle entre les ports (10 à 255 s), indiquez l'intervalle de pause que doit respecter le dispositif entre les ports.
5. Dans la section Display (Affichage), modifiez les options d'affichage par défaut pour la taille des miniatures et l'orientation de la division de la fenêtre Port Scan (Balayage des ports).
6. Cliquez sur OK.

Options d'affichage

View Toolbar (Afficher la barre d'outils)

Vous pouvez utiliser le Virtual KVM Client avec ou sans l’affichage de la barre d’outils.

Pour afficher et masquer la barre d’outils :

- Choisissez View > View Toolbar (Affichage > Afficher la barre d'outils).

View Status Bar (Afficher la barre d'état)

Par défaut, la barre d'état s'affiche au bas de la fenêtre cible.

Pour masquer la barre d'état :

- Cliquez sur View > Status Bar (Afficher > Barre d'état) pour la désélectionner.

Pour restaurer la barre d'état :

- Cliquez sur View > Status Bar (Afficher > Barre d'état) pour la sélectionner.

Scaling (Mise à l'échelle)

La mise à l’échelle de votre fenêtre cible permet d’afficher la totalité de l’écran du serveur cible. Cette fonction augmente ou réduit la taille de la vidéo cible pour qu’elle tienne dans la fenêtre du Virtual KVM Client et conserve le rapport hauteur/largeur de manière à permettre l’affichage de la totalité du bureau du serveur cible sans utiliser la barre de défilement.

Pour activer et désactiver la mise à l’échelle :

- Choisissez View > Scaling (Affichage > Mise à l'échelle).

Mode Full Screen (Mode Plein écran)

Lorsque vous passez au mode Plein écran, le plein écran de la cible s'affiche et utilise la même résolution que le serveur cible. Le raccourci-clavier utilisé pour quitter ce mode est spécifié dans la boîte de dialogue Options ; reportez-vous à ***Options d'outils*** (à la page 85).

En mode Plein écran, placez la souris au sommet de l'écran pour afficher la barre de menus du mode Plein écran. Pour que la barre de menus reste visible en mode Plein écran, activez l'option Pin Menu Toolbar (Epingler la barre d'outils de menu) de la boîte de dialogue Tool Options (Options d'outils). Reportez-vous à ***Options d'outils*** (à la page 85).

Pour entrer en mode Plein écran :

- Choisissez View > Full Screen (Affichage > Plein écran).

Pour quitter le mode Plein écran :

- Appuyez sur le raccourci clavier configuré dans la boîte de dialogue Options du menu Tools (Outils). Il s'agit par défaut de Ctrl+Alt+M.

Si vous souhaitez systématiquement accéder à la cible en mode Plein écran, désignez ce dernier comme mode par défaut.

Pour définir le mode Plein écran comme mode par défaut :

1. Cliquez sur Tools > Options (Outils > Options) pour ouvrir la boîte de dialogue Options.
2. Sélectionnez Enable Launch in Full Screen Mode (Activer le lancement en mode Plein écran) et cliquez sur OK.

Options d'aide

About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan)

Cette option de menu fournit les informations relatives à la version de Virtual KVM Client dans le cas où vous avez besoin de l'assistance technique de Raritan.

Pour obtenir les informations sur la version :

1. Sélectionnez Help > About Raritan Virtual KVM Client (Aide > A propos de Virtual KVM Client de Raritan).
2. Utilisez le bouton Copy to Clipboard (Copier dans le Presse-papiers) pour copier les informations contenues dans la boîte de dialogue dans un fichier de presse-papiers afin qu'elles soient accessibles ultérieurement lorsque vous communiquez avec le support (le cas échéant).

Multi-Platform Client (MPC)

Multi-Platform Client (MPC) de Raritan est une interface graphique utilisateur pour les lignes de produits Raritan qui permet un accès à distance aux serveurs cible connectés à Raritan KVM via des dispostifs IP. Pour plus d'informations sur l'utilisation de MPC, reportez-vous au **manuel des clients d'accès KVM et série** disponible sur le site Web de Raritan à la même page que le manuel d'utilisation. Des instructions sur le lancement de MPC sont fournies ici.

Notez que ce client est utilisé par divers produits Raritan. Aussi, des références à d'autres produits peuvent apparaître dans cette section de l'aide.

Lancement de MPC à partir d'un navigateur Web

Important : quel que soit le navigateur utilisé, vous devez autoriser l'affichage des fenêtres contextuelles à partir de l'adresse IP du dispositif Dominion pour lancer MPC.

Important : seuls Mac 10.5 et 10.6 avec un processeur Intel® peuvent exécuter JRE 1.6 et donc, être utilisés en tant que client. Mac 10.5.8 ne prend pas en charge MPC en tant que client autonome.

1. Pour ouvrir MPC à partir d'un client exécutant n'importe quel type de navigateur pris en charge, tapez http://ADRESSE-IP/mpc dans la ligne d'adresse, où ADRESSE-IP correspond à l'adresse IP de votre dispositif Raritan. MPC s'ouvre dans une nouvelle fenêtre.

   Remarque : la commande Alt+Tab permet de basculer entre des fenêtres sur le système local uniquement.

   Lorsque MPC s'ouvre, les dispositifs Raritan détectés automatiquement qui se trouvent sur votre sous-réseau s'affichent en arborescence dans le navigateur.

2. Si le nom de votre dispositif n'apparaît pas dans le navigateur, ajoutez-le manuellement :

   a. Choisissez Connection (Connexion) > New Profile (Nouveau profil). La fenêtre Add Connection (Ajouter une connexion) s'affiche.

   b. Entrez-y la description d'un dispositif, indiquez un type de connexion, ajoutez l'adresse IP du dispositif, puis cliquez sur OK. Vous pouvez modifier ces spécifications ultérieurement.

3. Dans le panneau de navigation situé à gauche de la page, double-cliquez sur l'icône qui correspond à votre dispositif Raritan pour vous y connecter.

Remarque : selon le navigateur utilisé et ses paramètres de sécurité, plusieurs vérifications de sécurité et de certificats, ainsi que des messages d'avertissement peuvent s'afficher. Vous devez accepter les options pour ouvrir MPC.

Remarque : si vous utilisez Firefox 3.0.3, vous pouvez rencontrer des problèmes de lancement de l'application. Si cela se produit, effacez la mémoire cache du navigateur et lancez l'application à nouveau.

Chapitre 4 Support virtuel

Dans ce chapitre

Présentation

La fonction Support virtuel prolonge les capacités KVM en permettant aux serveurs cible KVM d'accéder à distance aux supports des serveurs de fichiers de PC clients et réseau. LX prend en charge l'accès par support virtuel des disques durs et des images montées à distance.

Les modules d'interface pour ordinateur D2CIM-VUSB et D2CIM-DVUSB prennent en charge les sessions sur support virtuel pour les serveurs cible KVM disposant de l'interface USB 2.0. Ces CIM prennent également en charge Absolute Mouse Synchronization (synchronisation absolue de la souris) ainsi que la mise à jour du firmware à distance.

Les supports virtuels permettent d'effectuer des tâches à distance, telles que :

- le transfert de fichiers ;
- la réalisation de diagnostics ;
- l'installation ou la correction d'applications ;
- l'installation complète du système d'exploitation ;

Les types de supports virtuels sont pris en charge pour les clients Windows®, Mac® et Linux™ :

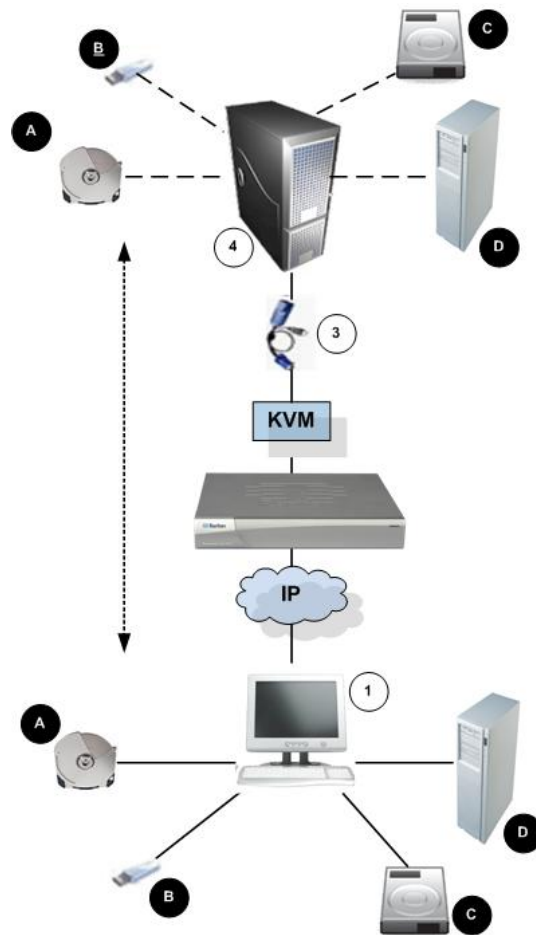
- lecteurs CD et DVD internes et montés sur USB ;
- dispositifs de stockage de masse USB ;
- disques durs de PC ;
- images ISO (images disque) ;

Remarque : ISO9660 est la norme prise en charge par Raritan. D'autres normes ISO peuvent cependant être utilisées.

Les systèmes d'exploitation clients suivants sont pris en charge :

- Windows
- Mac OS X 10.5
- Mac OS X 10.6
- Red Hat Desktop 4.0 et 5.0
- Open SUSE 10, 11
- Fedora 13 et 14

Virtual KVM Client (VKC) et Multi-Platform Client (MPC) peuvent être utilisés pour monter des types de supports virtuels, à l'exception de Mac OS X 10.5, qui est pris en charge exclusivement par MPC.



Légende			
1	Ordinateur de bureau	A	Lecteur CD/DVD
2	LX	B	Dispositif de stockage de masse USB
3	CIM	C	Disque dur de l'ordinateur
4	Serveur cible	D	Serveur de fichiers à distance (images ISO)

Conditions requises pour l'utilisation des supports virtuels

Grâce à la fonction de support virtuel, vous pouvez monter jusqu'à deux lecteurs (de différents types) pris en charge par le profil USB appliqué actuellement à la cible. Ces lecteurs sont accessibles pendant toute la durée de la session KVM.

Par exemple, vous pouvez monter un CD-ROM spécifique, l'utiliser puis le déconnecter lorsque vous avez terminé. Néanmoins, le « canal » du support virtuel CD-ROM demeure ouvert pour vous permettre de monter un autre CD-ROM virtuellement. Ces « canaux » de support virtuel restent ouverts jusqu'à la fermeture de la session KVM tant qu'elle est prise en charge par le profil USB.

Pour utiliser un support visuel, connectez/reliez-le au serveur de fichiers client ou réseau auquel vous souhaitez accéder à partir du serveur cible. Ce n'est pas nécessairement la première étape à effectuer, mais elle doit se dérouler avant de tenter d'accéder à ce support.

Pour utiliser les supports virtuels, les conditions suivantes doivent être remplies :

Dispositif Dominion

- Pour les utilisateurs ayant besoin d'accéder aux supports virtuels, des autorisations de dispositif doivent être définies pour permettre l'accès aux ports concernés, ainsi que l'accès aux supports virtuels pour ces ports (Autorisations des ports d'accès aux supports virtuels). Les permissions des ports sont définies au niveau du groupe.
- Il doit exister une connexion USB entre le dispositif et le serveur cible.
- Pour utiliser PC-Share, des paramètres de sécurité doivent également être activés sur la page Security Settings. **Facultatif**
- Vous devez choisir le profil USB correct pour le serveur cible KVM auquel vous vous connectez.

PC client

- Certaines options de support virtuel nécessitent des droits d'administrateur sur le PC client (par exemple, redirection de la totalité des lecteurs).

Remarque : si vous utilisez Microsoft Vista ou Windows 7, désactivez Contrôle de compte d'utilisateur ou sélectionnez Exécuter en tant qu'administrateur lorsque vous démarrez Internet Explorer. Pour cela, cliquez sur le menu Démarrer, recherchez Internet Explorer, cliquez dessus avec le bouton droit de la souris et sélectionnez Exécuter en tant qu'administrateur.

Serveur cible

- Les serveurs cible KVM doivent prendre en charge les lecteurs connectés USB.
- Tous les patchs récents doivent être installés sur les serveurs cible KVM qui exécutent Windows 2000.
- Les ports USB 2.0 sont plus rapides et donc préférables.

Supports virtuels dans un environnement Linux

Les informations importantes suivantes relatives à l'emploi des supports virtuels s'adressent aux utilisateurs Linux®.

Exigence en matière d'autorisation pour utilisateur racine

- Votre connexion au support virtuel peut être fermée si vous montez un CD-ROM depuis un client Linux à une cible, puis le démontez. La connexion se ferme également lorsqu'un lecteur de disquette a été monté et qu'une disquette est ensuite retirée. Pour éviter ces problèmes, vous devez être utilisateur racine.

Autorisations

Les utilisateurs doivent disposer des autorisations d'accès appropriées pour connecter le lecteur/CD-ROM à la cible. Pour vérifier si c'est le cas :

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0

brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

Dans l'exemple ci-dessus, l'autorisation doit être modifiée pour permettre l'accès en lecture.

Dans un système prenant en charge les LCA dans ses utilitaires de fichiers, la commande ls change de comportement de la manière suivante :

- Pour les fichiers dotés d'une LCA par défaut, ou d'une LCA contenant plus d'entrées que les trois LCA obligatoires, l'utilitaire Is(1) dans la forme longue produite par ls -l affiche un signe plus (+) après la chaîne d'autorisation.

Ceci est indiqué dans l'exemple fourni ici pour /dev/sr0, utilisez getfacl –a /dev/sr0 pour vérifier si l'accès a été accordé à l'utilisateur dans le cadre d'une LCA. C'est le cas ici et il peut donc connecter le cd-rom au serveur cible, même si la sortie de la commande ls –l peut indiquer le contraire.

```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl: Removing leading '/' from absolute path names
# file: dev/sr0
# owner: root
# group: cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

Une vérification similaire des autorisations concernant un dispositif amovible indique :

```
guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1


guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
&gt;  getfacl -a /dev/sdb1
getfacl: Removing leading '/' from absolute path names
# file: dev/sdb1
# owner: root
# group: disk
user::rw-
group::rw-
other::---
```

Ceci requiert que l'utilisateur reçoive des autorisations en lecture seule pour le dispositif amovible :

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

Le lecteur est alors disponible pour la connexion à la cible.

Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible

La fonction Lecture-écriture du support virtuel n'est pas disponible dans les situations suivantes :

- pour les clients Linux® et Mac®
- pour tous les disques durs
- lorsque le lecteur est protégé en écriture
- lorsque l'utilisateur ne dispose pas de l'autorisation de lecture-écriture :
  - l'accès aux autorisations d'accès aux ports est défini sur None (Aucun) ou View (Afficher)
  - l'accès des médias virtuels aux autorisations d'accès aux ports est défini sur Read-Only (Lecture seule) ou Deny (Refuser)

Utilisation des supports virtuels

Reportez-vous à ***Conditions requises pour l'utilisation des supports virtuels*** (à la page 97) avant d'utiliser le support virtuel.

Pour utiliser les supports virtuels :

1. Si vous souhaitez accéder à des images ISO de serveur de fichiers, identifiez ces images et ces serveurs de fichiers par le biais de la page Remote Console File Server Setup (Configuration des serveurs de fichiers de la console distante). Reportez-vous à ***Configuration du serveur de fichiers du support virtuel (Images ISO du serveur de fichiers uniquement)*** (à la page 102).

   Remarque : le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

2. Ouvrez une session KVM avec le serveur cible adéquat.
   a. Ouvrez la page Port Access (Accès aux ports) depuis la console distante.
   b. Connectez-vous au serveur cible à partir de la page Port Access (Accès aux ports) :
   - Cliquez sur le nom du port (Port Name) du serveur approprié.
   - Choisissez la commande Connect (Connecter) dans le menu d'action des ports. Le serveur cible s'ouvre dans une fenêtre Virtual KVM Client.
3. Connectez-vous au support virtuel.

Pour :	Sélectionnez cette option VM :
Lecteurs locaux	Connect Drive
Lecteurs de CD/DVD locaux	Connect CD-ROM/ISO (Connecter CD-ROM/ISO)
Images ISO	Connect CD-ROM/ISO (Connecter CD-ROM/ISO)
Images ISO de serveur de fichiers	Connect CD-ROM/ISO (Connecter CD-ROM/ISO)

Une fois vos tâches terminées, déconnectez le support virtuel. Reportez-vous à ***Déconnexion des supports virtuels*** (à la page 107).

Configuration du serveur de fichiers du support virtuel (Images ISO du serveur de fichiers uniquement)

Remarque : cette fonction est requise uniquement lors de l'utilisation de supports virtuels pour accéder aux images ISO du serveur de fichiers. le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

Remarque : La prise en charge de SMB/CIFS est requise sur le serveur de fichiers.

Utilisez la page File Server Setup (Configuration des serveurs de fichiers) de la console distante pour spécifier les serveurs de fichiers et les chemins d'accès aux images auxquelles vous souhaitez accéder à l'aide de la fonction Support virtuel. Les images ISO de serveurs de fichiers spécifiées ici sont disponibles dans les listes déroulantes Remote Server ISO Image Hostname (Nom d'hôte des images ISO de serveur distant) et Image de la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO des supports virtuels). Reportez-vous à ***Montage des images CD-ROM/DVD-ROM/ISO*** (à la page 105).

Pour désigner les images ISO de serveur de fichiers pour l'accès aux supports virtuels :

1. Sélectionnez Virtual Media (Supports virtuels) dans la console distante. La page File Server Setup (Configuration des serveurs de fichiers) s'ouvre.
2. Cochez la case Selected (Sélectionné) pour tous les supports qui seront accessibles comme supports virtuels.
3. Entrez les informations relatives aux images ISO de serveur de fichiers auxquelles vous souhaitez accéder :
   - IP Address/Host Name - Nom d'hôte ou adresse IP du serveur de fichiers.

- Image Path - Nom complet du chemin d'accès à l'emplacement de l'image ISO. Par exemple, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, etc.

Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

4. Cliquez sur Save (Enregistrer). Tous les supports indiqués ici peuvent maintenant être sélectionnés dans la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO des supports virtuels).

Remarque : vous ne pouvez pas accéder à une image ISO distante via les supports virtuels à l'aide d'une adresse IPv6 à cause des limites techniques du logiciel tiers utilisé par le dispositif LX, KX, KSX ou KX101 G2.

Remarque : si vous vous connectez à un serveur Windows 2003® et tentez de charger une image ISO du serveur, un message d'erreur peut s'afficher pour indiquer que le montage des supports virtuels sur le port a échoué, que la connexion au serveur est impossible, ou que le nom d'utilisateur et le mot de passe pour le serveur de fichiers sont incorrects. Dans ce cas, désactivez Serveur réseau Microsoft : communications signées numériquement.

Remarque : si vous vous connectez à un serveur Windows 2003 et tentez de charger une image ISO à partir de ce serveur, vous risquez de recevoir un message d'erreur indiquant : « Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password » (Echec du montage du support virtuel. Impossible de connecter le serveur de fichiers ou nom d'utilisateur et mot de passe du serveur de fichiers erroné). Dans ce cas, désactivez l'option Serveur réseau Microsoft : communications signées numériquement sur le serveur sous les stratégies Contrôleurs de domaine.

Connexion aux supports virtuels

Montage des lecteurs locaux

Cette option permet de monter un lecteur entier, ce qui signifie que le lecteur de disque entier est monté virtuellement sur le serveur cible. Utilisez-la uniquement pour les disques durs et les lecteurs externes. Ceux-ci ne comprennent pas les lecteurs réseau, CD-ROM ou DVD-ROM. Il s'agit de la seule option pour laquelle la fonction Read-Write (Lecture/écriture) est disponible.

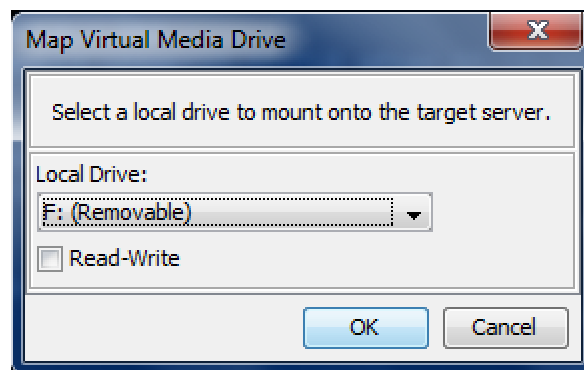
Remarque : les serveurs cible KVM exécutant certaines versions du système d'exploitation Windows risquent de ne pas accepter les nouvelles connexions de stockage en masse après la redirection vers eux d'une partition de format NTFS (par exemple, le disque C local).

Dans ce cas, fermez la console distante, puis reconnectez-vous avant de rediriger un autre dispositif de support virtuel. Si d'autres utilisateurs sont connectés au même serveur cible, ils doivent également fermer leurs connexions au serveur cible.

Remarque : dans KX II 2.1.0 (et supérieur), lorsque vous montez un lecteur externe, tel qu'un lecteur de disquettes, le voyant reste allumé parce que le dispositif vérifie le lecteur toutes les 500 millisecondes afin de s'assurer qu'il est toujours monté.

Pour accéder à un lecteur de l'ordinateur client :

1. Dans Virtual KVM Client, sélectionnez Virtual Media (Supports virtuels) > Connect Drive (Connecter le lecteur). La boîte de dialogue Map Virtual Media Drive (Mapper le lecteur de support virtuel) s'affiche. ()



2. Sélectionnez le lecteur dans la liste déroulante Local Drive (Lecteur local).

3. Pour disposer d'un accès en lecture et en écriture, cochez la case Read-Write (Lecture-écriture). Cette option est désactivée pour les lecteurs non amovibles. Reportez-vous à ***Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible*** (à la page 101) pour plus d'informations. Lorsque cette case est cochée, vous aurez accès en lecture et en écriture au disque USB connecté.

AVERTISSEMENT : l'activation de la fonction Lecture-écriture peut être dangereuse. L'accès simultané à un même lecteur à partir de plusieurs entités peut altérer les données. Si vous n'avez pas besoin d'un accès en écriture, ne sélectionnez pas cette option.

---

4. Cliquez sur Connect (Connecter). Le support est monté sur le serveur cible virtuellement. Vous pouvez y accéder de la même manière que pour tous les autres lecteurs.

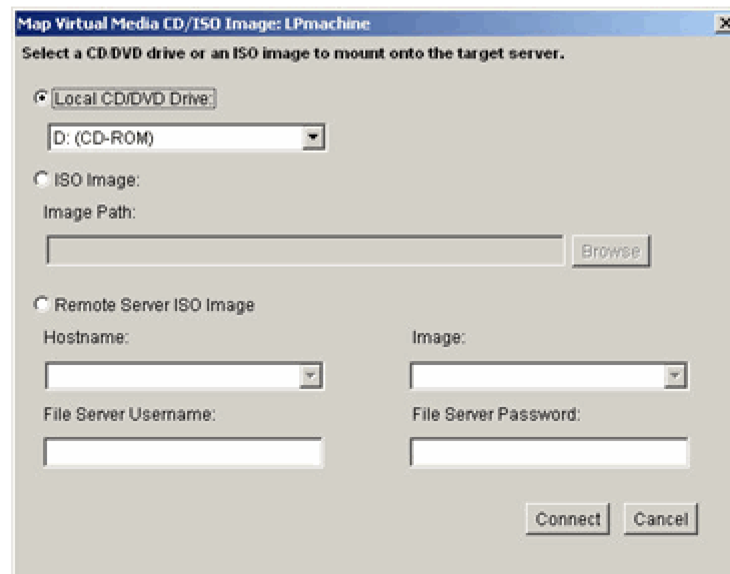
Montage des images CD-ROM/DVD-ROM/ISO

Cette option permet de monter des images ISO, CD-ROM et DVD-ROM.

Remarque : le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

▶ Pour accéder à une image ISO, CD-ROM ou DVD-ROM :

1. Dans Virtual KVM Client, sélectionnez Virtual Media > Connect CD-ROM/ISO Image (Supports virtuels > Connecter l'image ISO/CD-ROM). La boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image ISO/CD de support virtuel) s'affiche.



2. Pour les lecteurs de CD-ROM ou DVD-ROM internes et externes :

   a. Sélectionnez l'option Local CD/DVD Drive (Lecteur CD/DVD local).
   b. Sélectionnez le lecteur dans la liste déroulante Local CD/DVD Drive (Lecteur CD/DVD local). Tous les noms de lecteurs CD/DVD internes et externes sont générés dans la liste déroulante.
   c. Cliquez sur Connect (Connecter).
3. Pour les images ISO :
   a. Sélectionnez l'option ISO Image (Image ISO). Utilisez cette option lorsque vous souhaitez accéder à une image disque de CD, de DVD ou de disque dur. Le format ISO est le seul format pris en charge.
   b. Cliquez sur Browse (Parcourir).
   c. Localisez l'image disque que vous souhaitez utiliser, puis cliquez sur Open (Ouvrir). Le chemin d'accès est généré dans le champ Image Path (Chemin d'accès à l'image).
   d. Cliquez sur Connect (Connecter).
4. Pour les images ISO distantes d'un serveur de fichiers :
   a. Sélectionnez l'option Remote Server ISO Image (Image ISO de serveur à distance).
   b. Sélectionnez un nom d'hôte et une image dans la liste déroulante. Les chemins d'accès aux images et les serveurs de fichiers disponibles sont ceux que vous avez configurés via la page File Server Setup (Configuration des serveurs de fichiers). Seuls les éléments que vous avez configurés à l'aide de cette page figurent dans la liste déroulante.
   c. File Server Username - Nom d'utilisateur requis pour l'accès au serveur de fichiers. Le nom peut comprendre le nom du domaine, tel que mondomaine/nomutilisateur.
   d. File Server Password - Mot de passe requis pour l'accès au serveur de fichiers (le champ est masqué lorsque vous tapez).
   e. Cliquez sur Connect (Connecter).

   Le support est monté sur le serveur cible virtuellement. Vous pouvez y accéder de la même manière que pour tous les autres lecteurs.

Remarque : si vous travaillez avec des fichiers sur une cible Linux®, utilisez la commande Sync de Linux après la copie des fichiers à l'aide des supports virtuels afin d'afficher les fichiers copiés. Les fichiers risquent de ne pas apparaître si la synchronisation n'est pas effectuée.

Remarque : si vous utilisez le système d'exploitation Windows 7®, Disque amovible n'apparaît pas par défaut dans le dossier Poste de travail de Windows lorsque vous montez un lecteur de CD/DVD local, ou une image ISO locale ou distante. Pour afficher le lecteur de CD/DVD local, ou l'image ISO locale ou distante dans ce dossier, sélectionnez Outils > Options des dossiers > Affichage et désélectionnez Masquer les dossiers vides dans le dossier Ordinateur.

Remarque : vous ne pouvez pas accéder à une image ISO distante via les supports virtuels à l'aide d'une adresse IPv6 à cause des limites techniques du logiciel tiers.

Déconnexion des supports virtuels

► **Pour déconnecter les lecteurs de supports virtuels :**

- Pour les lecteurs locaux, sélectionnez Virtual Media (Supports virtuels) > Disconnect Drive (Déconnecter le lecteur).
- Pour les images ISO, CD et DVD, sélectionnez Virtual Media (Supports Virtuels) > Disconnect CD-ROM/ISO Image (Déconnecter l'image ISO/CD-ROM)

Remarque : outre la commande Disconnect (Déconnecter), la simple fermeture de la connexion KVM entraîne la déconnexion du support virtuel.

Chapitre 5 Gestion des utilisateurs

Dans ce chapitre

Groupes d'utilisateurs

LX stocke une liste interne de tous les noms des utilisateurs et des groupes pour déterminer les autorisations et permissions d'accès. Ces informations sont stockées de manière interne dans un format chiffré. Il existe plusieurs formes d'authentification et celle-ci est connue sous le nom d'authentification locale. Tous les utilisateurs doivent être authentifiés. Si LX est configuré pour LDAP/LDAPS ou RADIUS, cette authentification est traitée en premier, suivie par l'authentification locale.

Tous les dispositifs LX sont livrés avec trois groupes d'utilisateurs par défaut. Ces groupes ne peuvent être supprimés :

Utilisateur	Description
Admin	Les membres de ce groupe disposent de droits d'administrateur complets. L'utilisateur par défaut usine est membre de ce groupe et dispose de la totalité des droits de système. De plus, l'utilisateur Admin doit être membre du groupe Admin.
Unknown (Inconnu)	Il s'agit du groupe par défaut pour les utilisateurs authentifiés en externe à l'aide de LDAP/LDAPS ou RADIUS, ou que le système ne connaît pas. Si le serveur externe LDAP/LDAPS ou RADIUS ne peut pas identifier un groupe d'utilisateurs valide, le groupe Unknown est alors utilisé. De plus, tout utilisateur qui vient d'être créé est automatiquement affecté à ce groupe en attendant d'être transféré dans un autre.
Individual Group (Groupe individuel)	Un groupe individuel ne comporte en fait qu'un seul membre. Cet utilisateur spécifique est donc dans son propre groupe et non affilié à d'autres groupes réels. Les groupes individuels sont repérables par leur nom qui comporte le signe @. Le groupe individuel permet à un compte d'utilisateur de bénéficier des mêmes droits qu'un groupe.

Vous pouvez créer jusqu'à 254 groupes d'utilisateurs dans LX. Vous pouvez créer jusqu'à 254 groupes d'utilisateurs dans le LX.

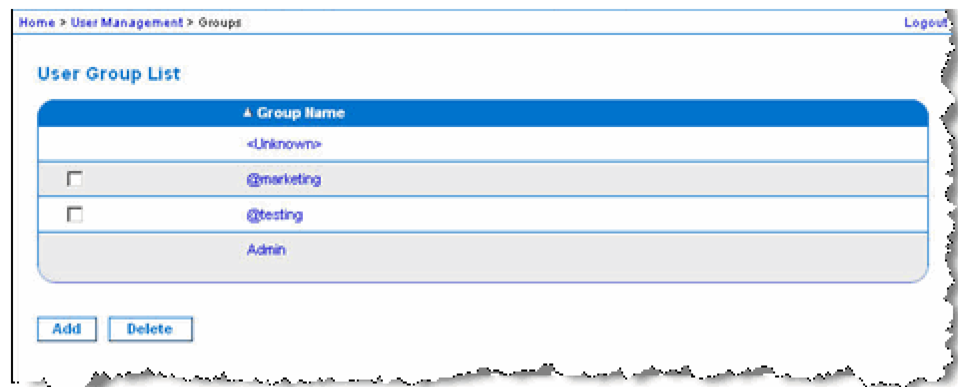
Liste des groupes d'utilisateurs

Les groupes d'utilisateurs sont utilisés avec une authentification à distance et locale (par l'intermédiaire de RADIUS ou de LDAP/LDAPS). Il est recommandé de définir les groupes avant de créer les différents utilisateurs car lorsque vous ajoutez un utilisateur, vous devez l'affecter à un groupe d'utilisateurs existant.

La page User Group List (Liste des groupes d'utilisateurs) affiche une liste de tous les groupes d'utilisateurs. Ceux-ci peuvent être triés dans l'ordre croissant ou décroissant en cliquant sur l'en-tête de colonne Group Name. A partir de la page User Group List, vous pouvez ajouter, modifier ou supprimer des groupes d'utilisateurs.

Pour répertorier les groupes d'utilisateurs :

- Sélectionnez User Management (Gestion des utilisateurs) > User Group List (Liste des groupes d'utilisateurs). La page User Group List s'ouvre.



Relation entre les utilisateurs et les groupes

Les utilisateurs appartiennent à un groupe et les groupes disposent de droits. La répartition en groupes des utilisateurs de votre unité LX offre un gain de temps, puisqu'elle permet de gérer les autorisations de l'ensemble des utilisateurs d'un groupe donné en une seule fois au lieu de les gérer individuellement.

Vous pouvez également choisir de ne pas associer des utilisateurs particuliers à des groupes. Vous avez alors la possibilité de classer l'utilisateur comme « individuel ».

Lorsqu'un utilisateur est authentifié, le dispositif utilise les informations relatives au groupe auquel il appartient pour déterminer ses autorisations : ports de serveur accessibles, autorisation éventuelle de redémarrer l'unité, etc.

Ajout d'un nouveau groupe d'utilisateurs

Pour ajouter un nouveau groupe d'utilisateurs :

1. Sélectionnez User Management > Add New User Group (Gestion des utilisateurs > Ajouter un nouveau groupe d'utilisateurs) ou cliquez sur Add (Ajouter) dans la page User Group List (Liste des groupes d'utilisateurs).
2. Entrez un nom descriptif pour le nouveau groupe d'utilisateurs dans le champ Group Name (64 caractères au plus).
3. Cochez les cases situées en regard des autorisations que vous souhaitez attribuer à tous les utilisateurs appartenant à ce groupe. Reportez-vous à ***Configuration des autorisations*** (à la page 111).
4. Cliquez sur OK.

Remarque : plusieurs fonctions d'administration sont disponibles dans MPC et à partir de la console locale de LX. Elles sont disponibles uniquement pour les membres du groupe par défaut Admin.

Home > User Management > Group

Group

Group Name *

▼ Permissions

Device Settings
Diagnostics
Maintenance
Modem Access
PC-Share
Security
User Management

▼ Port Permissions

Port	Access	VM Access
1: Dominion_LX_Port1	Deny	Deny
2: Dominion_LX_Port2	Deny	Deny
3: Dominion_LX_Port3	Deny	Deny
4: Dominion_LX_Port4	Deny	Deny
5: Dominion_LX_Port5	Deny	Deny
6: Dominion_LX_Port6	Deny	Deny
7: Dominion_LX_Port7	Deny	Deny
8: Dominion_LX_Port8	Deny	Deny
9: Dominion_LX_Port9	Deny	Deny
10: Dominion_LX_Port10	Deny	Deny
11: Dominion_LX_Port11	Deny	Deny
12: Dominion_LX_Port12	Deny	Deny
13: Dominion_LX_Port13	Deny	Deny
14: Dominion_LX_Port14	Deny	Deny
15: Dominion_LX_Port15	Deny	Deny
16: Dominion_LX_Port16	Deny	Deny

Set All to Deny
Set All to View
Set All to Control

Set All VM Access to Deny
Set All VM Access to Read-Only
Set All VM Access to Read-Write

OK Cancel

Configuration des autorisations

Important : la sélection de la case User Management (Gestion des utilisateurs) permet aux membres du groupe de modifier les autorisations de tous les utilisateurs, y compris les leurs. Accordez ces autorisations avec prudence.

Autorisation	Description
Device Settings (Paramètres du dispositif)	Paramètres réseau, paramètres date/heure, configuration des ports (nom de canal, etc.), gestion des événements (SNMP, Syslog),

Autorisation	Description
	configurations de serveur de fichiers du support virtuel.
Diagnostics	Etat d'interface réseau, statistiques de réseau, envoi d'une commande Ping à un hôte, tracer l'itinéraire jusqu'à un hôte, diagnostics de l'unité LX.
Maintenance	Sauvegarde et restauration de base des données, mise à niveau du firmware, réinitialisation des paramètres usine, redémarrage.
Modem Access (Accès par modem)	Autorisation d'utiliser le modem pour la connexion au dispositif LX.
PC-Share	Accès simultané à la même cible par plusieurs utilisateurs. Si vous utilisez une configuration multiniveau où un dispositif LX de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, tous les dispositifs doivent partager le même paramètre PC-Share. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.
Sécurité	Certificat SSL, paramètres de sécurité (VM Share, PC-Share).
Gestion des utilisateurs	Gestion des utilisateurs et des groupes, authentification à distance (LDAP/LDAPS/RADIUS), paramètres de connexion. Si vous utilisez une configuration multiniveau où un dispositif LX de base permet d'accéder à plusieurs autres dispositifs en niveau, les paramètres d'utilisateur, de groupe d'utilisateurs et d'authentification à distance doivent être cohérents à travers tous les dispositifs. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.

Configuration des autorisations d'accès aux ports

Pour chaque port de serveur, vous pouvez spécifier le type d'accès du groupe, ainsi que le type d'accès aux ports du support virtuel. Veuillez noter que le paramètre par défaut de toutes les autorisations est Deny (Refuser).

Port Access (Accès aux ports)	
option	**Description**
Deny (Refuser)	Accès refusé complètement
View (Afficher)	Afficher mais non interagir avec le serveur cible connecté
Control (Contrôler)	Contrôle le serveur cible connecté. Le contrôle doit être affecté au groupe si VM. Pour permettre à tous les utilisateurs d'un groupe de voir les commutateurs KVM ajoutés, un accès Control doit être accordé à chacun. S'ils ne disposent pas de cette autorisation et qu'un commutateur KVM est ajouté ultérieurement, ils ne pourront pas le voir.

VM access (Accès au support virtuel)	
option	**Description**
Deny (Refuser)	L'autorisation d'accès au support virtuel est totalement refusée pour le port.
Read-Only (Lecture seule)	L'accès au support virtuel est limité à l'accès en lecture uniquement.
Read-Write (Lecture-écriture)	Accès total (en lecture, en écriture) au support virtuel.

Si vous utilisez une configuration multiniveau où un dispositif LX de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, le dispositif en niveau applique des niveaux spécifiques de gestion des ports. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.

Définition des autorisations pour un groupe individuel

Pour configurer des autorisations attribuées à un groupe d'utilisateurs individuel :

1. Localisez le groupe parmi ceux qui figurent dans la liste. Les groupes individuels peuvent être identifiés par le signe @ présent dans le nom de groupe.
2. Cliquez sur Group Name (Nom du groupe). La page Group (Groupe) s'ouvre.
3. Sélectionnez les autorisations appropriées.
4. Cliquez sur OK.

Modification d'un groupe d'utilisateurs existant

Remarque : toutes les autorisations relatives au groupe Admin sont activées et ne peuvent pas être modifiées.

Pour modifier un groupe d'utilisateurs existant :

1. A partir de la page Group, modifiez les champs appropriés et définissez les autorisations adéquates.
2. Définissez les permissions pour le groupe. Cochez les cases situées en regard des permissions que vous souhaitez attribuer à tous les utilisateurs appartenant à ce groupe. Reportez-vous à ***Configuration des autorisations*** (à la page 111).
3. Définissez les autorisations d'accès aux ports. Spécifiez les ports de serveur auxquels peuvent accéder les utilisateurs appartenant à ce groupe (et le type d'accès). Reportez-vous à ***Configuration des autorisations d'accès aux ports*** (à la page 113).
4. Cliquez sur OK.

Pour supprimer un groupe d'utilisateurs :

Important : si vous supprimez un groupe contenant des utilisateurs, ces derniers sont automatiquement affectés au groupe d'utilisateurs <unknown> (inconnu).

Conseil : pour déterminer quels utilisateurs appartiennent à un groupe particulier, triez la User List (Liste des utilisateurs) par User Group (Groupe d'utilisateurs).

1. Sélectionnez un groupe parmi ceux qui figurent dans la liste en cochant la case située à gauche du nom de groupe.
2. Cliquez sur Delete (Supprimer).

3. Lorsque vous êtes invité à confirmer la suppression, cliquez sur OK.

Utilisateurs

Les utilisateurs doivent disposer de noms d'utilisateur et de mots de passe pour accéder à LX. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre unité LX. Vous pouvez créer jusqu'à 254 utilisateurs pour chaque groupe.

Si vous utilisez une configuration multiniveau où un dispositif LX de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, les utilisateurs auront besoin d'autorisations d'accès au dispositif de base et à chaque dispositif en niveau (selon les besoins). Lorsqu'un utilisateur se connecte au dispositif de base, chaque dispositif en niveau est interrogé et l'utilisateur peut accéder à chaque serveur cible pour lequel il dispose d'autorisations. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.

Liste des utilisateurs

La page User List (Liste des utilisateurs) affiche une liste de tous les utilisateurs, avec leur nom d'utilisateur, leur nom complet et le groupe d'utilisateurs auquel ils appartiennent. Pour trier cette liste en fonction d'une colonne, cliquez sur le nom de celle-ci. A partir de la page User List, vous pouvez également ajouter, modifier ou supprimer des utilisateurs.

Pour afficher la liste des utilisateurs :

- Sélectionnez User Management (Gestion des utilisateurs) > User List (Liste des utilisateurs). La page User List (Liste des utilisateurs) s'ouvre.

Home > User Management > Users Logou

User List

	▲ Username	Full Name	User Group
	admin	Admin	Admin
☐	marketing	Addie Consumer	@marketing
☐	tester	Joe Tester	@tester

Add Delete Force User Logoff

Ajout d'un nouvel utilisateur

Il est recommandé de définir les groupes d'utilisateurs avant de créer des utilisateurs LX, car lorsque vous ajoutez un utilisateur, vous devez l'affecter à un groupe d'utilisateurs existant. Reportez-vous à **Ajout d'un nouveau groupe d'utilisateurs** (à la page 110).

Vous pouvez ajouter de nouveaux utilisateurs, modifier leurs informations et réactiver des utilisateurs sur la page User.

Remarque : un nom d'utilisateur peut être désactivé lorsque le nombre de tentatives de connexion qui ont échoué a atteint la limite définie dans la page Security Settings (Paramètres de sécurité). Reportez-vous à Paramètres de sécurité.

Pour ajouter un nouvel utilisateur :

1. Sélectionnez User Management > Add New User (Gestion des utilisateurs > Ajouter un nouvel utilisateur) ou cliquez sur Add (Ajouter) dans la page User List (Liste des utilisateurs).
2. Tapez un nom unique dans le champ Username (Nom d'utilisateur) (16 caractères au maximum).
3. Tapez le nom complet de la personne dans le champ Full Name (Nom complet) (64 caractères au maximum).
4. Tapez un mot de passe dans le champ Password, puis entrez-le à nouveau dans le champ Confirm Password (Confirmer le mot de passe) (64 caractères au maximum).
5. Choisissez un groupe dans la liste déroulante User Group (Groupe d'utilisateurs).

   Si vous ne souhaitez pas affecter cet utilisateur à un groupe d'utilisateurs existant, sélectionnez Individual Group (Groupe individuel) dans la liste déroulante. Pour plus d'informations sur les autorisations associées à un groupe individuel, reportez-vous à ***Définition des autorisations pour un groupe individuel*** (à la page 114).
6. Pour activer le nouvel utilisateur, laissez la case Active cochée. Cliquez sur OK.

Modification d'un utilisateur existant

Pour modifier un utilisateur existant :

1. Ouvrez la page User List (Liste des utilisateurs) en choisissant User Management (Gestion des utilisateurs) > User List.
2. Localisez l'utilisateur parmi ceux répertoriés sur la page User List.
3. Cliquez sur le nom d'utilisateur. La page User (Utilisateur) s'ouvre.

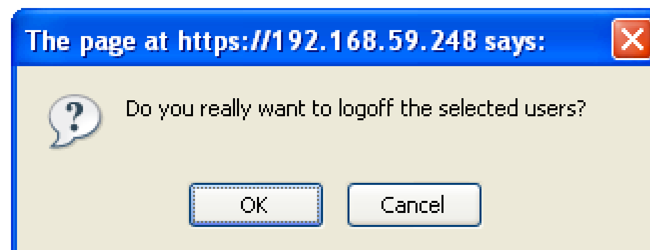
4. Sur la page User (Utilisateur), modifiez les champs appropriés. Reportez-vous à ***Ajout d'un nouvel utilisateur*** (à la page 116) pour plus d'informations sur les méthodes d'accès à la page User.
5. Pour supprimer un utilisateur, cliquez sur Delete. Vous êtes invité à confirmer la suppression.
6. Cliquez sur OK.

Déconnexion d'un utilisateur (Déconnexion forcée)

Si vous êtes administrateur, vous pouvez déconnecter un autre utilisateur authentifié localement qui est connecté à LX.

Pour déconnecter un utilisateur :

1. Ouvrez la page User List en choisissant User Management > User List ou cliquez sur le lien Connected User (Utilisateur connecté) dans le panneau gauche de la page.
2. Recherchez l'utilisateur parmi ceux répertoriés sur la page User List et cochez la case en regard de son nom.
3. Cliquez sur Force User Logoff (Forcer la déconnexion de l'utilisateur).
4. Cliquez sur OK dans la boîte de dialogue Logoff User (Déconnecter l'utilisateur) pour forcer la déconnexion.



5. Un message de confirmation indique alors que l'utilisateur est déconnecté. Ce message contient les date et heure de la déconnexion. Cliquez sur OK pour fermer ce message.

Paramètres d'authentification

L'authentification est un processus qui consiste à vérifier l'identité d'un utilisateur. Une fois l'utilisateur authentifié, son groupe permet de déterminer ses autorisations d'accès aux ports et au système. Les droits accordés à l'utilisateur déterminent le type d'accès autorisé. Cela s'appelle l'autorisation.

Lorsque LX est configuré pour l'authentification à distance, le serveur d'authentification externe est utilisé principalement à des fins d'authentification et non d'autorisation.

Si vous utilisez une configuration multiniveau où un dispositif LX de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, le dispositif de base et les dispositifs en niveau doivent utiliser les mêmes paramètres d'authentification.

Sur la page Authentication Settings (Paramètres d'authentification), vous pouvez configurer le type d'authentification utilisé pour l'accès à LX.

Remarque : lorsque l'authentification à distance (LDAP/LDAPS ou RADIUS) est sélectionnée, si l'utilisateur est introuvable, la base de données d'authentification locale est également vérifiée.

Pour configurer l'authentification :

1. Choisissez User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification). La page Authentication Settings s'ouvre :
2. Choisissez le protocole d'authentification que vous souhaitez utiliser (Local Authentication [Authentification locale], LDAP/LDAPS ou RADIUS). L'option LDAP active les champs LDAP restants ; l'option RADIUS active les champs RADIUS restants.
3. Si vous sélectionnez Local Authentication (Authentification locale), passez à l'étape 6.
4. Si vous sélectionnez LDAP/LDAPS, lisez la section intitulée Implémentation de l'authentification à distance LDAP pour obtenir des informations sur la façon de renseigner les champs dans la section LDAP de la page Authentication Settings (Paramètres d'authentification).
5. Si vous sélectionnez RADIUS, lisez la section intitulée Implémentation de l'authentification à distance RADIUS pour obtenir des informations sur la façon de renseigner les champs dans la section RADIUS de la page Authentication Settings (Paramètres d'authentification).
6. Cliquez sur OK pour enregistrer.

Pour réinitialiser les paramètres par défaut usine :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

Implémentation de l'authentification à distance LDAP/LDAPS

LDAP (Lightweight Directory Access Protocol, protocole allégé d'accès à un annuaire) est un protocole de mise en réseau pour la recherche et la modification de services d'annuaires fonctionnant sur TCP/IP. Un client démarre une session LDAP en se connectant à un serveur LDAP/LDAPS (le port TCP par défaut est 389). Le client envoie ensuite les demandes de fonctionnement au serveur, et le serveur envoie les réponses en retour.

Rappel : Microsoft Active Directory fonctionne de manière native comme serveur d'authentification LDAP/LDAPS.

Pour utiliser le protocole d'authentification LDAP :

1. Cliquez sur User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification) pour ouvrir la page Authentication Settings.
2. Sélectionnez le bouton radio LDAP pour activer la section LDAP de la page.
3. Cliquez sur l'icône ► LDAP pour développer la section LDAP de la page.

   Configuration du serveur

4. Dans le champ Primary LDAP Server (Serveur LDAP principal), entrez l'adresse IP ou le nom DNS de votre serveur d'authentification à distance LDAP/LDAPS (256 caractères au plus). Lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) est sélectionnée avec l'option Enable LDAPS Server Certificate Validation (Activer la validation du certificat du serveur LDAPS), le nom DNS doit être utilisé pour vérifier le certificat du serveur LDAP du CN.
5. Dans le champ Secondary LDAP Server (Serveur LDAP secondaire), entrez l'adresse IP ou le nom DNS de votre serveur de sauvegarde LDAP/LDAPS (256 caractères au plus). Lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) sélectionnée, le nom DNS doit être utilisé. Notez que les champs restants comportent les mêmes paramètres que le champ Primary LDAP Server. **Facultatif**
6. Type de serveur LDAP externe.
7. Sélectionnez le serveur LDAP/LDAPS externe. Sélectionnez-le parmi les options disponibles :
   - Serveur LDAP générique.

- Microsoft Active Directory. Active Directory est une implémentation des services d'annuaires LDAP/LDAPS par Microsoft à utiliser dans les environnements Windows.

8. Entrez le nom du domaine Active Directory si vous avez sélectionné Microsoft Active Directory. Par exemple, *acme.com*. Consultez l'administrateur Active Directory pour obtenir un nom de domaine spécifique.
9. Dans le champ User Search DN (ND de recherche d'utilisateur), entrez le ND de l'emplacement dans la base de données LDAP où la recherche d'informations d'utilisateur doit commencer. Vous pouvez entrer jusqu'à 64 caractères. Exemple de valeur de recherche de base : `cn=Users,dc=raritan,dc=com`. Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ces champs.
10. Entrez le Distinguished Name de l'utilisateur administratif dans le champ DN of Administrative User (64 caractères au plus). Renseignez ce champ si votre serveur LDAP autorise uniquement les administrateurs à rechercher des informations d'utilisateur à l'aide du rôle Administrative User. Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ce champ. Exemple de valeur de ND d'utilisateur administratif : `cn=Administrator,cn=Users,dc=testradius,dc=com`. **Facultatif**

11. Si vous avez entré un Distinguished Name pour l'utilisateur administratif, vous devez entrer le mot de passe qui sera utilisé pour authentifier le ND de l'utilisateur administratif par comparaison avec le serveur d'authentification à distance. Entrez le mot de passe dans le champ Secret Phrase (Expression secrète) et à nouveau dans le champ Confirm Secret Phrase (Confirmer l'expression secrète) (128 caractères au plus).

Authentication Settings

Local Authentication

LDAP

RADIUS

▼ LDAP

Server Configuration

Primary LDAP Server

192.168.59.187

Secondary LDAP Server (optional)

192.168.51.214

Type of External LDAP Server

Microsoft Active Directory

Active Directory Domain

testradius.com

User Search DN

cn=users,dc=testradius,dc=com

DN of Administrative User (optional)

cn=Administrator,cn=users,dc=testrac

Secret Phrase of Administrative User

●●●●●●●●●

Confirm Secret Phrase

LDAP/LDAP Secure (LDAP/LDAP sécurisé)

12. Cochez la case Enable Secure LDAP (Activer le LDAP sécurisé) si vous souhaitez utiliser SSL. Ceci coche la case Enable LDAPS Server Certificate Validation (Activer la validation du certificat du serveur LDAPS). SSL (Secure Sockets Layer) est un protocole cryptographique qui permet à LX de communiquer en toute sécurité avec le serveur LDAP/LDAPS.
13. Le port par défaut est 389. Utilisez le port LDAP TCP standard ou spécifiez un autre port.

14. Le port LDAP sécurisé par défaut est 636. Utilisez le port par défaut ou spécifiez un autre port. Ce champ est utilisé uniquement lorsque la case Enable Secure LDAP (Activer le LDAP sécurisé) est cochée.
15. Cochez la case Enable LDAPS Server Certificate Validation afin d'utiliser le fichier de certificat de l'autorité de certification (AC) racine téléversé précédemment pour valider le certificat fourni par le serveur. Si vous ne souhaitez pas utiliser le fichier de certificat, désactivez la case à cocher. Désactiver cette fonction revient à accepter un certificat signé par une autorité de certification inconnue. Cette case à cocher est uniquement disponible lorsque la case Enable Secure LDAP est cochée.

Remarque : lorsque l'option Enable LDAPS Server Certificate Validation est sélectionnée, outre l'utilisation du certificat de l'AC racine pour la validation, le nom d'hôte du serveur doit correspondre au nom commun fourni dans le certificat du serveur.

16. Le cas échéant, téléversez le fichier de certificat de l'AC racine. Ce champ est activé lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) est sélectionnée. Consultez l'administrateur de votre serveur d'authentification pour obtenir le fichier de certificat de l'AC au format Base64 codé X-509 pour le serveur LDAP/LDAPS. Utilisez Browse (Parcourir) pour accéder au fichier du certificat. Si vous remplacez un certificat pour un serveur LDAP/LDAPS par un nouveau, vous devez redémarrer LX pour que ce nouveau certificat prenne effet.

LDAP / Secure LDAP
Enable Secure LDAP
Port
389
Secure LDAP Port
636
Enable LDAPS Server Certificate Validation
Root CA Certificate File
Browse...
Upload
Note: Reboot device after certificate file is uploaded.

Test LDAP Server Access (Test de l'accès à un serveur LDAP)

Raritan.

17. LX permet de tester la configuration LDAP dans la page Authentication Settings (Paramètres d'authentification) à cause de la difficulté à configurer correctement le serveur LDAP et LX pour l'authentification à distance. Pour tester la configuration LDAP, entrez le nom et le mot de passe de connexion dans les champs Login for testing (Nom de connexion pour le test) et Password for testing (Mot de passe pour le test) respectivement. Il s'agit des nom d'utilisateur et de mot de passe entrés pour accéder à LX et que le serveur LDAP utilisera pour vous authentifier. Cliquez sur Test.

    Une fois le test terminé, un message s'affiche pour indiquer si le test a réussi ou s'il a échoué, un message d'erreur détaillé apparaît. Un message de réussite ou détaillé d'erreur, en cas d'échec, apparaît. Il donne également des informations de groupe extraites du serveur LDAP distant pour l'utilisateur du test en cas de réussite.

Test LDAP Server Access

Login for testing

Password for testing

Test

Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory

LX prend en charge l'authentification des utilisateurs auprès d'Active Directory® (AD) sans qu'il soit nécessaire de définir les utilisateurs localement au niveau de LX. Les comptes et mots de passe des utilisateurs Active Directory peuvent ainsi être gérés exclusivement sur le serveur AD. L'autorisation et les droits des utilisateurs AD sont contrôlés et administrés par le biais de stratégies classiques dans LX et de droits appliqués localement à des groupes d'utilisateurs AD.

IMPORTANT : si vous êtes déjà client de Raritan, Inc. et que vous avez configuré le serveur Active Directory en modifiant le schéma AD, LX continue de prendre en charge cette configuration et il ne vous est pas nécessaire d'effectuer les opérations suivantes. Pour obtenir des informations sur la mise à jour du schéma AD LDAP/LDAPS, reportez-vous à ***Mise à jour du schéma LDAP*** **(à la page 234).**

▶ Pour activer le serveur AD sur LX :

1. A l'aide de LX, créez des groupes spéciaux et attribuez-leur les autorisations et privilèges appropriés. Par exemple, créez des groupes tels que KVM_Admin et KVM_Operator.

2. Sur le serveur Active Directory, créez des groupes portant le même nom qu'à l'étape précédente.
3. Sur votre serveur AD, affectez les utilisateurs de l'unité LX aux groupes créés au cours de l'étape 2.
4. A partir de LX, activez et configurez le serveur AD comme il se doit. Reportez-vous à ***Implémentation de l'authentification à distance LDAP/LDAPS*** (à la page 119).

Remarques importantes :

- Le nom de groupe est sensible à la casse.
- LX fournit les groupes par défaut suivants qui ne peuvent pas être modifiés ni supprimés : Admin et <Unknown (Inconnu)>. Vérifiez que le serveur Active Directory n'utilise pas les mêmes noms de groupe.
- Si les informations de groupe renvoyées par le serveur Active Directory ne correspondent pas à une configuration de groupe LX, ce dernier attribue automatiquement le groupe <Unknown> (Inconnu) aux utilisateurs qui ont réussi à s'authentifier.
- Si vous utilisez un numéro de rappel, vous devez entrer la chaîne sensible à la casse suivante : *msRADIUSCallbackNumber.*
- D'après les recommandations de Microsoft, il vaut mieux utiliser les groupes globaux avec les comptes d'utilisateurs, non les groupes locaux de domaines.

Implémentation de l'authentification à distance RADIUS

RADIUS (Remote Authentication Dial-in User Service) est un protocole d'authentification, d'autorisation et de gestion destiné aux applications d'accès aux réseaux.

▶ Pour utiliser le protocole d'authentification RADIUS :

1. Cliquez sur User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification) pour ouvrir la page Authentication Settings.
2. Cliquez sur le bouton radio RADIUS pour activer la section RADIUS de la page.
3. Cliquez sur l'icône ▸ RADIUS pour développer la section RADIUS de la page.
4. Dans les champs Primary Radius Server (Serveur Radius principal) et Secondary Radius Server (Serveur Radius secondaire), entrez l'adresse IP des serveurs d'authentification à distance principal et secondaire facultatif, respectivement (256 caractères au plus).
5. Dans les champs Shared Secret (Secret partagé), entrez le secret du serveur utilisé pour l'authentification (128 caractères au plus).

Le secret partagé est constitué d'une chaîne de caractères devant être connus à la fois par LX et le serveur RADIUS afin de leur permettre de communiquer en toute sécurité. C'est en fait un mot de passe.

6. La valeur par défaut Authentication Port (Port d'authentification) est 1812 mais peut être modifiée si nécessaire.
7. La valeur par défaut Accounting Port (Port de gestion) est 1813 mais peut être modifiée si nécessaire.
8. La valeur Timeout (Délai d'attente) est enregistrée en secondes et le délai d'attente par défaut est 1 seconde, mais peut être modifiée si nécessaire.

   Le délai d'attente correspond au laps de temps utilisé par LX pour obtenir une réponse du serveur RADIUS avant d'envoyer une autre requête d'authentification.
9. Le nombre de tentatives par défaut est 3.

   Il s'agit du nombre de tentatives accordées à LX pour envoyer une requête d'authentification au serveur RADIUS.
10. Sélectionnez une option dans la liste déroulante Global Authentication Type (Type d'authentification globale) :
    - PAP - Avec le protocole PAP, les mots de passe sont envoyés en texte brut. Le protocole PAP n'est pas interactif. Le nom d'utilisateur et le mot de passe sont envoyés en un ensemble unique de données une fois la connexion établie, et non sous la forme d'une invite de connexion suivie de l'attente d'une réponse.

- CHAP - Avec le protocole CHAP, l'authentification peut être demandée par le serveur à tout moment. Le protocole CHAP est plus sûr que le protocole PAP.

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication
LDAP
RADIUS

► LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Secondary RADIUS Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Global Authentication Type
PAP

OK | Reset To Defaults | Cancel

Cisco ACS 5.x pour l'authentification RADIUS

Si vous utilisez un serveur Cisco ACS 5.x, effectuez les opérations suivantes sur celui-ci après avoir configuré LX pour l'authentification RADIUS.

Remarque : les opérations suivantes incluent les menus et les options Cisco utilisés pour accéder à chaque page. Reportez-vous à la documentation Cisco pour obtenir les informations les plus récentes sur chaque opération et plus de détails sur leur exécution.

- Ajoutez LX en tant que client AAA (**obligatoire**) - Network Resources > Network Device Group > Network Device and AAA Clients (Ressources réseau > Groupe de dispositifs réseau > Dispositif réseau et clients AAA).
- Ajoutez/modifiez les utilisateurs (**obligatoire**) - Network Resources > Users and Identity Stores > Internal Identity Stores > Users (Ressources réseau > Utilisateurs et magasins d'identités > Magasins d'identités internes > Utilisateurs).
- Configurez l'accès réseau par défaut pour activer le protocole CHAP (**facultatif**) - Policies > Access Services > Default Network Access (Stratégies > Services d'accès > Accès réseau par défaut).
- Créez des règles de stratégie d'autorisation pour contrôler l'accès (**obligatoire**) - Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles (Eléments de stratégie > Autorisation et permissions > Accès réseau > Profils d'autorisation).
  - Type de dictionnaire : RADIUS-IETF
  - Attribut RADIUS : Filter-ID
  - Type d'attribut : Chaîne
  - Attribute Value: Raritan:G{KVM_Admin} (où KVM_Admin est le nom du groupe créé localement sur le commutateur KVM Dominion KVM). Sensible à la casse.
- Configurez les conditions de sessions (date et heure) (**obligatoire**) - Policy Elements > Session Conditions > Date and Time (Eléments de stratégie > Conditions de session > Date et heure).
- Configurez/créez la stratégie d'autorisation d'accès réseau (**obligatoire**) - Access Policies > Access Services > Default Network Access>Authorization (Stratégies d'accès > Services d'accès > Accès réseau par défaut > Autorisation).

Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS

Lorsqu'une demande d'authentification RADIUS est acceptée, LX détermine les autorisations accordées à un utilisateur donné en fonction des autorisations du groupe auquel il appartient.

Votre serveur RADIUS distant peut fournir ces noms de groupes d'utilisateurs en retournant un attribut, implémenté comme FILTER-ID (ID FILTRE) RADIUS. Le format du FILTER-ID (ID FILTRE) doit être le suivant : Raritan:G{*NOM_GROUPE*} où *NOM_GROUPE* est une chaîne indiquant le nom du groupe auquel l'utilisateur appartient.

```
Raritan:G{NOM_GROUPE}:D{Numéro de rappel}
```

ou NOM_GROUPE est une chaîne indiquant le nom du groupe auquel appartient l'utilisateur et Numéro de rappel est le numéro associé au compte de l'utilisateur dont le modem LX se servira pour rappeler le compte de l'utilisateur.

Spécifications des échanges de communication RADIUS

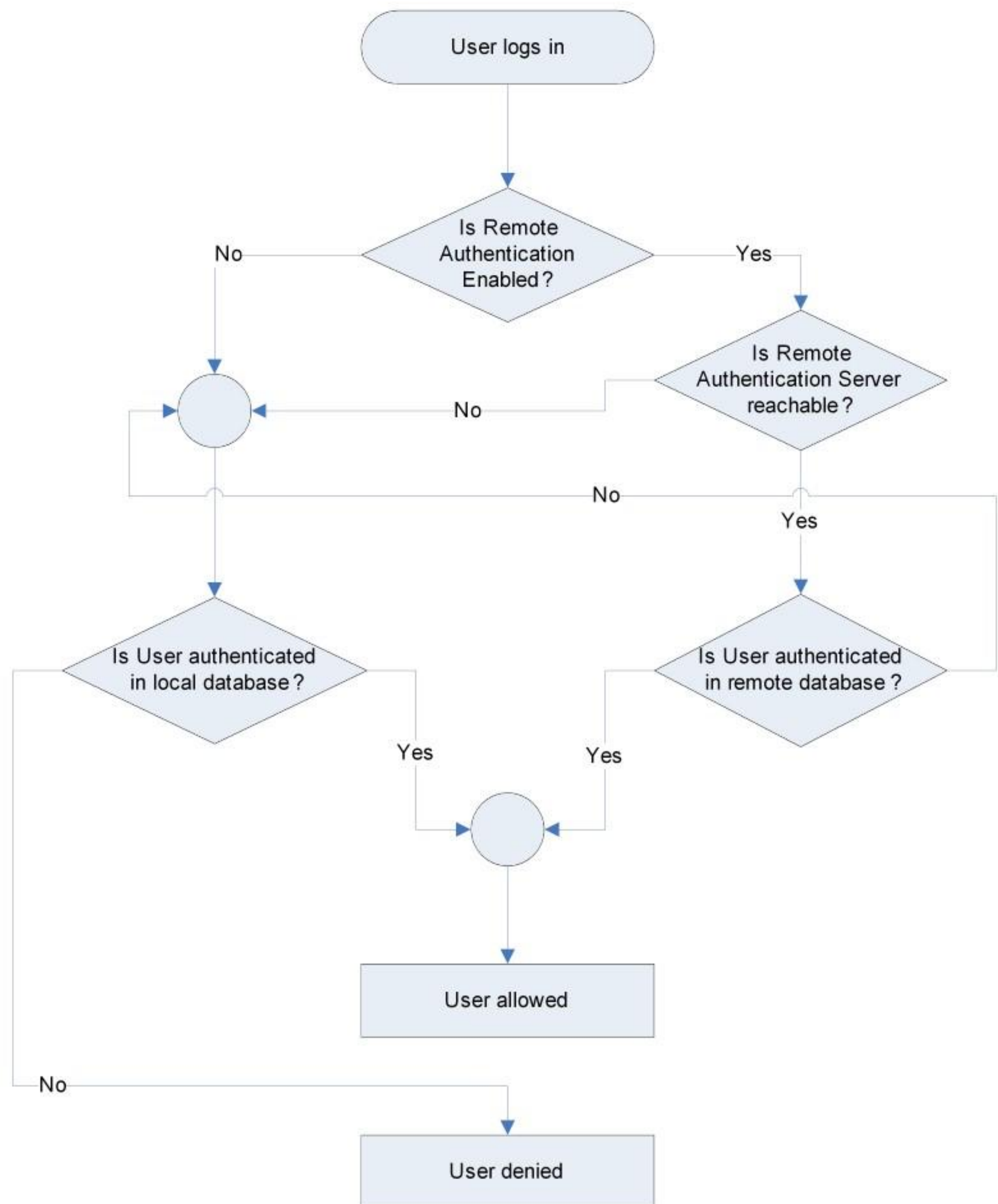
LX envoie les attributs RADIUS suivants à votre serveur RADIUS :

Attribut	Données
Connexion	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-IP-Address (4)	Adresse IP de LX.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.
User-Password(2)	Mot de passe chiffré.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Démarre la gestion.
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0.
NAS-IP-Address (4)	Adresse IP de LX.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.

Attribut Déconnexion	Données
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Met fin à la gestion.
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0.
NAS-IP-Address (4)	Adresse IP de LX.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.

Processus d'authentification de l'utilisateur

L'authentification à distance suit le processus défini dans le diagramme ci-dessous :



Modification d'un mot de passe

Pour modifier votre mot de passe :

1. Sélectionnez User Management (Gestion des utilisateurs) > Change Password (Modifier le mot de passe). La page Change Password (Modifier le mot de passe) s'ouvre.
2. Entrez votre mot de passe actuel dans le champ Old Password (Ancien mot de passe).
3. Entrez un nouveau mot de passe dans le champ New Password. Retapez-le dans le champ Confirm New Password (Confirmer le nouveau mot de passe). Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques et caractères spéciaux (présents sur un clavier anglais).
4. Cliquez sur OK.
5. Vous recevrez confirmation que le mot de passe a bien été changé. Cliquez sur OK.

Remarque : si des mots de passe sécurisés sont utilisés, cette page affiche des informations sur le format requis pour ces mots de passe. Pour plus d'informations sur les mots de passe et les mots de passe sécurisés, reportez-vous à **Mots de passe sécurisés** *(à la page 161).*

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK Cancel

Chapitre 6 Gestion des dispositifs

Dans ce chapitre

Paramètres réseau

Utilisez la page Network Settings (Paramètres réseau) pour personnaliser la configuration du réseau (par exemple, adresse IP, port de détection et paramètres de l'interface LAN) de votre unité LX.

Deux options permettent de paramétrer votre configuration IP :

- None (Néant) (valeur par défaut) : il s'agit de l'option recommandée (IP statique). Comme LX fait partie intégrante de l'infrastructure de votre réseau, vous ne voulez probablement pas que son adresse IP change fréquemment. Cette option vous permet de définir les paramètres de réseau.
- DHCP : avec cette option, l'adresse IP est automatiquement attribuée par un serveur DHCP.

Pour modifier la configuration de réseau :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Mettez à jour les paramètres réseau de base. Reportez-vous à ***Paramètres réseau de base*** (à la page 133).
3. Mettez à jour les paramètres relatifs à l'interface LAN. Reportez-vous à Paramètres de l'interface LAN.
4. Cliquez sur OK pour confirmer ces configurations. Si vos modifications nécessitent le redémarrage du dispositif, un message de redémarrage apparaît.

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

Paramètres réseau de base

Ces procédures décrivent comment affecter une adresse IP sur la page Network Settings (Paramètres réseau). Pour obtenir des informations complètes sur tous les champs ainsi que sur le fonctionnement de cette page, reportez-vous à ***Paramètres réseau*** (à la page 132).

Pour affecter une adresse IP :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Indiquez un nom de dispositif significatif pour votre unité LX. 32 caractères alphanumériques au plus, avec des caractères spéciaux valides et aucun espace.
3. Dans la section IPv4, entrez ou sélectionnez les paramètres réseau spécifiques à IPv4 appropriés :
   a. Entrez l'adresse IP si nécessaire. L'adresse IP par défaut est 192.168.0.192.
   b. Entrez le masque de sous-réseau. Le masque de sous-réseau par défaut est 255.255.255.0.
   c. Entrez la passerelle par défaut si None (Néant) est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).
   d. Entrez le nom d'hôte DHCP préféré si DHCP est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).
   e. Sélectionnez la configuration IP automatique. Les options suivantes sont disponibles :
   - None (Static IP) (Néant (IP statique)) : cette option nécessite que vous indiquiez manuellement les paramètres réseau.

     Cette option est recommandée car LX est un dispositif d'infrastructure et son adresse IP ne doit pas être modifiée.
   - DHCP : le protocole de configuration d'hôte dynamique est utilisé par les ordinateurs mis en réseau (clients) pour obtenir des adresses IP uniques et d'autres paramètres à partir du serveur DHCP.

     Avec cette option, les paramètres réseau sont attribués par le serveur DHCP. Si DHCP est utilisé, entrez le nom d'hôte préféré (DHCP uniquement). Maximum de 63 caractères.
4. Si IPv6 doit être utilisé, entrez ou sélectionnez les paramètres réseau spécifiques à IPv6 appropriés dans la section IPv6 :
   a. Cochez la case IPv6 pour activer les champs de la section.
   b. Renseignez le champ Global/Unique IP Address (Adresse IP globale/unique). Il s'agit de l'adresse IP affectée à LX.

c. Renseignez le champ Prefix Length (Longueur de préfixe). Il s'agit du nombre de bits utilisés dans l'adresse IPv6.

d. Renseignez le champ Gateway IP Address (Adresse IP de la passerelle).

e. Link-Local IP Address (Adresse IP Lien-local). Cette adresse est attribuée automatiquement au dispositif. Elle est utilisée pour la détection de voisins ou en l'absence de routeurs. **Read-Only (Lecture seule)**

f. Zone ID. Ce champ identifie le dispositif auquel l'adresse est associée. **Read-Only (Lecture seule)**

g. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :

- None (Néant) - Utilisez cette option si vous ne souhaitez pas de configuration IP automatique et préférez définir l'adresse IP vous-même (IP statique). Cette option par défaut est recommandée.

  Lorsqu'elle est sélectionnée pour la configuration IP automatique, les champs Network Basic Settings (Paramètres réseau de base) sont activés : Global/Unique IP Address (Adresse IP globale/unique), Prefix Length (Longueur de préfixe) et Gateway IP Address (Adresse IP de la passerelle). Vous pouvez paramétrer manuellement la configuration IP.

- Router Discovery (Détection de routeur) - Utilisez cette option pour affecter automatiquement des adresses IPv6 ayant une portée « Global » ou « Unique Local » au-delà des adresses « Link Local » qui ne s'appliquent qu'à un sous-réseau connecté directement.

5. Sélectionnez Obtain DNS Server Address Automatically (Obtenir l'adresse du serveur DNS automatiquement) si DHCP est sélectionné et que l'option Obtain DNS Server Address (Obtenir l'adresse du serveur DNS) est activée. Si l'option When Obtain DNS Server Address Automatically est sélectionnée, les données DNS fournies par le serveur DHCP seront utilisées.

6. Si l'option Use the Following DNS Server Addresses (Utiliser les adresses de serveur DNS suivantes) est sélectionnée, indépendamment de la sélection de DHCP ou non, les adresses entrées dans cette section seront utilisées pour la connexion au serveur DNS.

   Entrez les données suivantes si l'option Use the Following DNS Server Addresses est sélectionnée. Il s'agit des adresses DNS principale et secondaire qui seront utilisées si la connexion au serveur DNS principal est perdue en raison d'une panne.

   a. Primary DNS Server IP Address (Adresse IP du serveur DNS principal)

   b. Secondary DNS Server IP Address (Adresse IP du serveur DNS secondaire)

7. Lorsque vous avez terminé, cliquez sur OK.

Reportez-vous à Paramètres de l'interface LAN pour plus d'informations sur la configuration de cette section de la page Network Settings (Paramètres réseau).

Remarque : dans certains environnements, le paramètre par défaut du champ LAN Interface Speed & Duplex (Vitesse d'interface LAN & Duplex), Autodetect (auto-détection), ne définit pas correctement les paramètres réseau, ce qui entraîne des problèmes sur le réseau. Dans ce cas, paramétrez le champ LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN) de LX sur 100 Mbps/Full Duplex (Bidirectionnel simultané) (ou toute option appropriée à votre réseau) pour résoudre le problème. Reportez-vous à la page **Paramètres réseau** *(à la page 132) pour plus d'informations.*

Paramètres de l'interface LAN

Les paramètres actuels sont identifiés dans le champ Current LAN interface parameters (Paramètres actuels de l'interface LAN).

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Renseignez le champ LAN Interface Speed & Duplex (Vitesse et duplex de l'interface LAN) en sélectionnant une des options suivantes :
   - Autodetect (Détection automatique) (option par défaut)
   - 10 Mbps/Half - Les deux témoins clignotent.
   - 10 Mbps/Full - Les deux témoins clignotent.
   - 100 Mbps/Half - Le témoin jaune clignote.
   - 100 Mbps/Full - Le témoin jaune clignote.
   - 1000 Mbps/Full (gigabit) - Le témoin vert clignote.
   - Half-duplex permet la communication dans les deux directions, mais seulement une direction à la fois (non simultanément).
   - Full-duplex permet la communication dans les deux directions simultanément.

   Remarque : des problèmes surviennent parfois lors de l'exécution à 10 Mbps en half duplex ou en full duplex. Dans ce cas, essayez un autre paramètre de vitesse et de duplex.

   Reportez-vous à ***Paramètres de vitesse réseau*** (à la page 232) pour plus d'informations.
3. Sélectionnez la bande passante.
4. Cliquez sur OK pour appliquer les paramètres LAN.

Services du dispositif

La page Device Services vous autorise à configurer les fonctions suivantes :

- activer l'accès SSH
- activer la fonction multiniveau pour le LX de base
- entrer le port de détection
- activer l'accès direct aux ports
- activer la fonction de validation du certificat du serveur de téléchargement AKC si vous utilisez AKC

Activation de SSH

Activez l'accès SSH pour permettre aux administrateurs d'accéder à LX via l'application SSH v2.

Pour activer l'accès SSH :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Cochez la case Enable SSH Access.
3. Renseignez le champ SSH Port. Le numéro de port TCP SSH standard est 22 mais ce numéro peut être changé pour offrir un niveau supérieur d'opérations de sécurité.
4. Cliquez sur OK.

Paramètres des ports HTTP et HTTPS

Vous pouvez configurer les ports HTTP et/ou HTTPS utilisés par l'unité LX. Par exemple, si vous utilisez le port HTTP 80 par défaut pour autre chose, le remplacement du port garantit que le dispositif ne tentera pas de l'utiliser.

Pour modifier les paramètres des ports HTTP et/ou HTTPS :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Entrez les nouveaux ports dans les champs HTTP Port et/ou HTTPS Port.
3. Cliquez sur OK.

Saisie du port de détection

La détection de LX s'effectue sur un port TCP unique et configurable. Le port par défaut est le port 5000 mais vous pouvez configurer ce paramètre de manière à utiliser le port TCP de votre choix à l'exception des ports 80 et 443. Pour accéder à LX par-delà un pare-feu, les paramètres du pare-feu doivent permettre la communication bidirectionnelle par l'intermédiaire du port 5000 par défaut ou d'un autre port configuré ici.

Pour activer le port de détection :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Renseignez le champ Discovery Port (Port de détection).

3. Cliquez sur OK.

Configuration et activation de la fonction multiniveau

LX et la fonction multiniveau générique sont pris en charge par LX. La fonction multiniveau vous permet d'accéder aux cibles LX par l'intermédiaire d'un dispositif LX de base.

Remarque : les dispositifs de base et en niveau doivent tous utiliser la même version de firmware.

Des dispositifs peuvent être ajoutés et supprimés d'une configuration selon les besoins, pour obtenir un maximum de deux niveaux étagés.

Lors du paramétrage des dispositifs, vous utiliserez des CIM spécifiques pour des configurations particulières. Reportez-vous à ***Fonction multiniveau - Types de cibles, CIM pris en charge et mise en niveau de configurations*** (à la page 140) pour obtenir une description des cibles pouvant être incluses à une configuration multiniveau, et des informations sur la compatibilité des CIM et la configuration des dispositifs.

Avant d'ajouter des dispositifs en niveau, vous devez activer la fonction multiniveau pour le dispositif de base et les dispositifs en niveau. L'activation des dispositifs de base s'effectue sur la page Device Settings (Paramètres du dispositif). L'activation des dispositifs en niveau s'effectue sur la page Local Port Settings (Paramètres du port local). Une fois les dispositifs activés et configurés, ils apparaissent sur la page Port Access (Accès aux ports) (***Page Port Access*** (à la page 47)).

Lorsque LX est configuré pour servir de dispositif de base ou en niveau, il apparaît comme suit :

- Configured As Base Device (Configuré comme dispositif de base) dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'interface du LX pour les dispositifs de base.
- Configured As Tier Device (Configuré comme dispositif en niveau) dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'interface du LX pour les dispositifs en niveau.
- Le dispositif de base sera identifié par Base dans le panneau gauche de l'interface du dispositif en niveau sous Connect User (Utilisateur connecté).
- Les connexions cible vers un port en niveau depuis la base seront affichés sous la forme de 2 ports connectés.

Le dispositif de base fournit un accès à distance et local via une liste de ports consolidée de la page Port Access. Les dispositifs en niveau offrent un accès à distance depuis leur propre liste de ports. L'accès local n'est pas disponible sur les dispositifs en niveau lorsque la fonction multiniveau est activée.

La configuration des ports, notamment la modification du nom du CIM, doit être effectuée directement depuis chaque dispositif. Elle ne peut pas être effectuée depuis le dispositif de base pour les ports de cibles en niveau.

La fonction multiniveau prend également en charge les commutateurs KVM pour alterner entre les serveurs. Reportez-vous à ***Configuration des commutateurs KVM*** (à la page 152).

Activation de la fonction multiniveau

Connectez depuis un port de serveur cible sur le dispositif de base aux ports vidéo/clavier/souris du port Local Access du LX en niveau à l'aide d'un D2CIM-DVUSB.

Pour activer la fonction multiniveau :

1. Depuis la base du niveau, choisissez Device Settings > Device Services (Paramètres du dispositif > Services du dispositif). La page de paramétrage Device Services (Services du dispositif) apparaît.
2. Sélectionnez Enable Tiering as Base (Activer la fonction multiniveau comme base).
3. Dans le champ Base Secret (Secret de la base), entrez le secret partagé entre la base et les dispositifs en niveau. Ce secret est exigé pour permettre aux dispositifs en niveau d'authentifier le dispositif de base. Vous entrerez le même mot secret pour le dispositif en niveau.
4. Cliquez sur OK.
5. Activez les dispositifs en niveau. Depuis le dispositif en niveau, choisissez Device Settings > Local Port Settings (Paramètres du dispositif > Paramètres du port local).
6. Dans la section Enable Local Ports (Activer les ports locaux) de la page, sélectionnez Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local).
7. Dans le champ Tier Secret (Secret du niveau), entrez le mot secret entré pour le dispositif de base sur la page Device Settings (Paramètres du dispositif).
8. Cliquez sur OK.

Fonction multiniveau - Types de cibles, CIM pris en charge et mise en niveau de configurations

La configuration des ports, notamment la modification du nom du CIM, doit être effectuée directement depuis chaque dispositif. Elle ne peut pas être effectuée depuis le dispositif de base pour les ports de cibles en niveau.

Fonctions non prises en charge et limitées sur les cibles en niveau

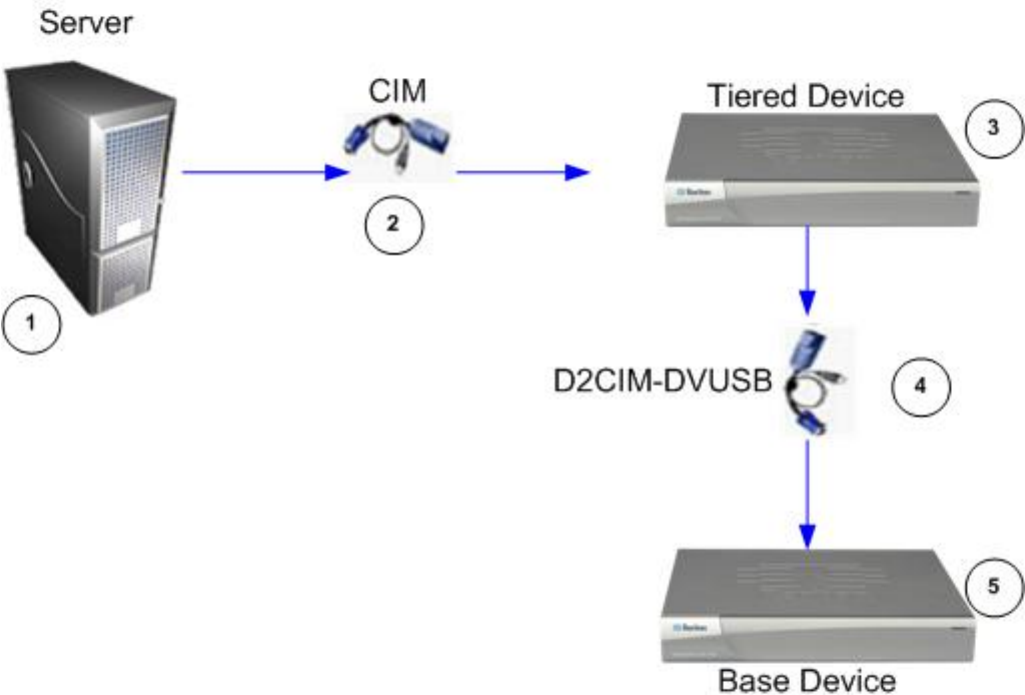
Les fonctions suivantes ne sont pas prises en charge sur les cibles en niveau :

- Dispositifs en niveau de support virtuel
- MCCAT comme dispositif en niveau

Exemple de câble dans les configurations multiniveaux

Le diagramme suivant illustre les configurations de câblage entre un dispositif en niveau LX et un dispositif de base LX.

Connectez depuis un port de serveur cible sur le dispositif de base aux ports vidéo/clavier/souris du port Local Access du LX en niveau à l'aide d'un D2CIM-DVUSB.



Légende	
1	Serveur cible
2	CIM du serveur cible au dispositif en niveau LX

Légende	
3	Dispositif en niveau LX
4	CIM D2CIM-DVUSB du dispositif en niveau LX au dispositif de base LX
5	Dispositif de base LX

Activation d'un accès direct aux ports via URL

L'accès direct aux ports permet aux utilisateurs de ne pas avoir à passer par la boîte de dialogue de connexion et par la page d'accès aux ports du dispositif. Cette fonction permet également d'entrer un nom d'utilisateur et un mot de passe directement et d'accéder à la cible si le nom d'utilisateur et le mot de passe ne sont pas contenus dans l'URL.

Des données d'URL importantes concernant l'accès direct aux ports suivent :

Si vous utilisez VKC et l'accès direct aux ports :

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

Si vous utilisez AKC et l'accès direct aux ports :

- https://IPaddress/dpa.asp?username=nom d'utilisateur&password=mot de passe&port=numéro de port&client=akc

Où :

- Nom d'utilisateur et mot de passe sont facultatifs. S'ils ne sont pas fournis, une boîte de dialogue de connexion apparaît et, après avoir été authentifié, l'utilisateur est connecté directement à la cible.
- Le port peut être un numéro ou un nom de port. Si vous utilisez un nom de port, il doit être unique ou une erreur est signalée. Si le port est totalement omis, une erreur est signalée.
- Client=akc est facultatif sauf si vous utilisez un client AKC. Si client=akc n'est pas inclus, VKC est utilisé comme client.

Pour activer l'accès direct aux ports :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.

2. Cochez la case Enable Direct Port Access via URL (Activer l'accès direct aux ports via URL) pour accorder aux utilisateurs un accès direct à une cible via le dispositif Dominion par transmission des paramètres nécessaires dans l'URL.
3. Cliquez sur OK.

Activation de la validation du certificat du serveur de téléchargement AKC

Si vous utilisez le client AKC, vous pouvez décider d'utiliser ou non la fonction Enable AKC Download Server Certificate Validation (Activer la validation du certificat du serveur de téléchargement AKC).

Option 1 : Ne pas activer la validation du certificat du serveur de téléchargement AKC (paramètre par défaut)

Si vous n'activez pas la validation du certificat du serveur de téléchargement AKC, tous les utilisateurs de dispositifs Dominion doivent :

- Vérifiez que les cookies de l'adresse IP du dispositif auquel vous accédez ne sont pas bloqués.
- Les utilisateurs de serveurs Windows Vista, Windows 7 et Windows 2008 doivent s'assurer que l'adresse IP du dispositif auquel ils accèdent est incluse dans la zone Sites approuvés de leur navigateur et que le mode protégé n'est pas activé lors de l'accès au dispositif.

Option 2 : Activer la validation du certificat du serveur de téléchargement AKC

Si vous activez la validation du certificat du serveur de téléchargement AKC :

- Les administrateurs doivent téléverser un certificat valide sur le dispositif ou générer un certificat auto-signé sur celui-ci. Le certificat doit désigner un hôte valide.
- Chaque utilisateur doit ajouter le certificat AC (ou une copie du certificat auto-signé) dans la liste Autorités de certification racines de confiance de leur navigateur.

▶ Pour installer le certificat auto-signé dans les systèmes d'exploitation Windows Vista® et Windows 7® :

1. Ajoutez l'adresse IP de LX dans la zone Site de confiance et assurez-vous que le mode protégé est désactivé.
2. Lancez Internet Explorer® en indiquant comme URL l'adresse IP de LX. Un message Erreur de certificat apparaît.
3. Sélectionnez Afficher les certificats.

4. Sur l'onglet Général, cliquez sur Installer le certificat. Le certificat est alors installé dans la liste Autorités de certification racines de confiance.
5. Une fois le certificat installé, l'adresse IP de LX peut être supprimé de la zone Site de confiance.

► **Pour activer la validation du certificat du serveur de téléchargement AKC :**

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Vous pouvez cocher la case Enable AKC Download Server Certificate Validation ou laisser la fonction désactivée (valeur par défaut).
3. Cliquez sur OK.

Configuration des paramètres de modem

► **Pour configurer les paramètres de modem :**

1. Cliquez sur Device Settings (Paramètres du dispositif) > Modem Settings (Paramètres de modem) pour ouvrir la page Modem Settings.
2. Cochez la case Enable Modem (Activer le modem). Les champs Serial Line Speed (Vitesse de la ligne série) et Modem Init String (Chaîne initiale du modem) sont activés.
3. Le champ Serial Line Speed du modem est paramétré sur 115200.
4. Renseignez le champ Modem Init String. Si la chaîne du modem est laissée vide, la chaîne suivante est envoyée par défaut au modem : ATZ OK AT OK.

   Cette information est utilisée pour configurer les paramètres du modem. Comme chaque modem paramètre ces valeurs à sa manière, ce document n'indique pas comme définir ces valeurs. L'utilisateur doit se référer au modem pour créer la chaîne appropriée.

   a. Paramètres de modem :

- Activation du contrôle de flux RTS/CTS (demande pour émettre/prêt à émettre)
- Envoi de données à l'ordinateur dès la réception de RTS
- CTS devrait être configuré de manière à abandonner uniquement lorsque le contrôle de flux le demande.
- DTR devrait être configuré pour les réinitialisations de modem avec basculement DTR.
- DSR devrait toujours être activé.
- DCD devrait être configuré comme étant activé après la détection d'un signal porteur. (DCD ne devrait être activé que lorsque la connexion du modem est établie avec le côté distant.)

5. Renseignez le champ Modem Server IPv4 Address (Adresse IPv4 du serveur de modem) et le champ Modem Client IPv4 Address (Adresse IPv4 du client de modem).

Remarque : les adresses IP des client et serveur du modem doivent provenir du même sous-réseau et ne peuvent pas chevaucher le sous-réseau LAN du dispositif.

6. Cliquez sur OK pour appliquer vos changements ou sur Reset to Defaults (Restaurer les paramètres par défaut) pour rétablir les valeurs par défaut des paramètres.

Reportez-vous à ***Modems certifiés*** (à la page 227) pour plus d'informations sur les modems certifiés qui fonctionnent avec LX. Pour plus d'informations sur les paramètres qui permettront les meilleures performances lors de la connexion à LX par modem, reportez-vous à **Création, modification et suppression des profils dans MPC - Dispositifs de la deuxième génération** dans le **manuel des clients d'accès KVM et série**.

Remarque : l'accès direct par modem à l'interface HTML de LX n'est pas prise en charge. Vous devez utiliser le MPC autonome pour accéder à LX par modem.

Configuration des paramètres de date et heure

La page Date/Time Settings (Paramètres de date/heure) permet d'indiquer la date et l'heure de LX. Il existe deux méthodes pour ce faire :

- Définir la date et l'heure manuellement ou
- les synchroniser avec un serveur NTP.

Pour définir la date et l'heure :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Date/Time (Date/heure). La page Date/Time Settings (Paramètres de date/heure) s'ouvre.
2. Sélectionnez votre fuseau horaire dans la liste déroulante Time Zone (Fuseau horaire).
3. Pour prendre en compte l'heure d'été, cochez la case Adjust for daylight savings time (Régler selon les changements d'heure).
4. Choisissez la méthode que vous souhaitez utiliser pour définir la date et l'heure :
   - User Specified Time - Sélectionnez cette option pour saisir la date et l'heure manuellement. Pour l'option User Specified Time (Heure spécifiée par l'utilisateur), entrez la date et l'heure. Pour l'heure, utilisez le format hh:mm (système de 24 heures).
   - Synchronize with NTP Server - Sélectionnez cette option pour synchroniser la date et l'heure avec le serveur NTP.
5. Pour l'option Synchronize with NTP Server (Synchroniser avec le serveur NTP) :
   a. Entrez une adresse IP dans le champ Primary Time server (Serveur d'horloge principal).
   b. Renseignez le champ Secondary Time server (Serveur d'horloge secondaire). **Facultatif**

6. Cliquez sur OK.

Home > Device Settings > Date/Time Settings

Date/Time Settings

Time Zone

(GMT -05:00) US Eastern

Adjust for daylight savings time

User Specified Time

Date (Month, Day, Year)

May 09 , 2008

Time (Hour, Minute)

10 : 18

Synchronize with NTP Server

Primary Time server

Secondary Time server

OK Reset To Defaults Cancel

Gestion des événements

La fonction de gestion des événements de LX permet d'activer et de désactiver la distribution des événements système aux gestionnaires SNMP, Syslog et au journal d'audit.

Configuration de la gestion des événements - Paramètres

Configuration SNMP

Le protocole SNMP est un protocole simplifié de gestion de réseau qui prend en charge la gestion de réseau et la surveillance des dispositifs réseau, ainsi que leurs fonctions. LX offre la prise en charge de l'agent SNMP via la fonction Event Management (Gestion des événements).

► **Pour configurer SNMP (permettre la journalisation de SNMP) :**

1. Sélectionnez Device Settings (Paramètres du dispositif) > Event Management - Settings (Gestion des événements - Paramètres). La page Event Management - Settings (Gestion des événements - Paramètres) s'ouvre.
2. Cochez la case SNMP Logging Enabled (Journalisation SNMP activée). Les champs SNMP restants sont activés.
3. Dans les champs Name (Nom), Contact et Location (Emplacement), tapez le nom de l'agent SNMP (soit celui du dispositif) tel qu'il apparaît dans l'interface de la console LX, un contact associé à ce dispositif et l'emplacement physique du dispositif Dominion.
4. Renseignez le champ Agent Community String (Chaîne de communauté de l'agent) (chaîne du dispositif). La communauté SNMP est le groupe auquel appartiennent les dispositifs et les postes de gestion exécutant SNMP. Elle permet de définir l'emplacement où les données sont envoyées. Le nom de la communauté est utilisé pour identifier le groupe. Le dispositif ou l'agent SNMP peuvent appartenir à plusieurs communautés SNMP.
5. Indiquez si la communauté est en lecture seule ou en lecture-écriture à l'aide de la liste déroulante Type.
6. Configurez jusqu'à cinq gestionnaires SNMP en indiquant leurs IP de destination/nom d'hôte, numéro de port et communauté.
7. Cliquez sur le lien « Click here to view the Dominion SNMP MIB » (Cliquez ici pour afficher le MIB SNMP du dispositif Dominion) pour accéder à la base des données de gestion SNMP.
8. Cliquez sur OK.

► **Pour configurer Syslog (activer le transfert Syslog) :**

1. Cochez la case Enable Syslog Forwarding (Activer le transfert Syslog) pour consigner les messages du dispositif sur un serveur Syslog distant.
2. Entrez l'adresse IP/le nom d'hôte de votre serveur Syslog dans le champ IP Address (Adresse IP).
3. Cliquez sur OK.

Pour restaurer les paramètres d'usine par défaut :

- Cliquez sur Reset To Defaults (Restaurer les paramètres par défaut).

Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

Home > Device Settings > Event Management - Settings

SNMP Configuration

☐ SNMP Logging Enabled

Name
LX

Contact

Location

Agent Community String

Type
Read-Only

Destination IP/Hostname	Port #	Community
	162	public
	162	public
	162	public
	162	public
	162	public

Click here to view the Dominion LX SNMP MIB

SysLog Configuration

☐ Enable Syslog Forwarding

IP Address/Host Name

OK | Reset To Defaults | Cancel

Configuration des ports

La page Port Configuration (Configuration des ports) affiche la liste des ports de l'unité LX. Les ports connectés aux serveurs cible KVM sont affichés en bleu. Pour les ports sans CIM connecté ou pour lesquels le nom de CIM est vide, un nom de port par défaut Dominion-LX_Port# est attribué, où Port# est le numéro du port physique de LX.

Lorsque le statut d'un port est désactivé, Not Available (Non disponible) apparaît comme statut. Un port peut être désactivé lorsque son CIM a été retiré ou mis hors tension.

Une fois le port renommé, utilisez Reset to Default (Restaurer les paramètres par défaut) à tout moment pour rétablir le nom du port par défaut.

Pour accéder à la configuration d'un port :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.

   Cette page est affichée initialement par ordre de numéros de port, mais elle peut être triée sur n'importe quel champ en cliquant sur son en-tête de colonne.

   - Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif LX.
   - Port Name - Nom attribué au port. Ou, renommez les ports non connectés à LX via un CIM et donc, dotés du statut Not Available (Non disponible). Pour renommer un port dont le statut est Not Available, effectuez une des opérations suivantes :
     - Renommez le port. Lorsqu'un CIM est connecté, son nom est utilisé.
     - Renommez le port et sélectionnez Persist name on Next CIM Insertion (Conserver le nom pour l'insertion de CIM suivante). Lorsqu'un CIM est connecté, le nom qui a été affecté sera copié dans le CIM.
     - Réinitialisez le port, nom inclus, aux valeurs par défaut usine en sélectionnant Reset to Defaults. Lorsqu'un CIM est connecté, son nom est utilisé.

   Remarque : n'utilisez pas d'apostrophe pour le nom de port (CIM).

   - Port Type (Type de port) :

- DCIM - CIM Dominion
- Not Available (Non disponible) - Aucun CIM connecté
- MCUTP - Master Console MCUTP, CIM dans un câble
- PCIM - CIM Paragon
- Dual - VM - CIM de support virtuel (D2CIM-VUSB et D2CIM-DVUSB)
- KVM Switch (Commutateur KVM) - Connexion au commutateur KVM générique

2. Cliquez sur le nom du port que vous souhaitez modifier. La page Port pour KVM s'ouvre.

Configuration des serveurs cible standard

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 29) pour obtenir une description de la connexion de l'équipement.
2. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
3. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
4. Sélectionnez Standard KVM Port comme sous-type du port.
5. Attribuez un nom au serveur connecté à ce port. Ce nom peut contenir jusqu'à 32 caractères alphanumériques et spéciaux.
6. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
7. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.
8. Cliquez sur OK.

Configuration des commutateurs KVM

LX autorise les connexions en niveau aux commutateurs KVM analogiques génériques prenant en charge la commutation par raccourci-clavier. Diverses séquences de raccourci-clavier KVM sont fournies à la sélection. Sélectionnez-en une pour l'associer à la séquence de raccourci-clavier prise en charge sur le commutateur KVM analogique connecté via ce port. Les cibles figurant sur le commutateur KVM analogique en niveau pourront ainsi être accessibles depuis la liste de regroupement de ports de la page Port Access.

Important : pour permettre aux groupes d'utilisateurs de voir le commutateur KVM que vous créez, vous devez d'abord créer le commutateur, puis le groupe. Si un groupe d'utilisateurs existant doit voir le commutateur KVM que vous créez, vous devez créer à nouveau le groupe d'utilisateurs.

Pour configurer des commutateurs KVM :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
3. Sélectionnez KVM Switch.
4. Sélectionnez le modèle de commutateur KVM (KVM Switch Model).

   Remarque : un commutateur seulement apparaîtra dans la liste déroulante.

5. Sélectionnez la séquence de raccourcis-clavier du commutateur KVM (KVM Switch Hot Key Sequence).
6. Entrez le nombre maximum de ports cible (2 à 32).
7. Dans le champ KVM Switch Name, entrez le nom à utiliser pour faire référence à cette connexion de port.
8. Activez les cibles auxquelles la séquence de raccourcis-clavier de commutateur KVM sera appliquée. Indiquez les ports de commutateur KVM auxquels des cibles sont reliées en sélectionnant Active pour chacun des ports.
9. Dans la section KVM Managed Links (Liens gérés de KVM) de la page, vous pouvez configurer la connexion à une interface de navigateur Web si elle est disponible.

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL Name - Entrez l'URL de l'interface.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

e. Username Field - Entrez le paramètre username qui sera utilisé dans l'URL. Par exemple *username*=admin, où *username* est le champ username.

f. Password Field - Entrez le paramètre password qui sera utilisé dans l'URL. Par exemple, *password*=raritan, où *password* est le champ password.

10. Cliquez sur OK.

Pour modifier le statut actif d'un port ou d'une URL de commutateur KVM :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
3. Désactivez la case à cocher Active en regard du port ou de l'URL cible de commutateur KVM pour modifier son statut actif.
4. Cliquez sur OK.

Configuration des paramètres du port local de LX

A partir de la page de paramétrage du port local, vous avez la possibilité de personnaliser de nombreux paramètres de la console locale de LX, notamment le clavier, les raccourcis-clavier, le délai de commutation de l'écran, le mode d'économie d'alimentation, les paramètres de résolution de l'interface utilisateur locale et l'authentification d'utilisateur locale.

▶ Pour configurer les paramètres du port local :

Remarque : certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage doit se produire lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

1. Sélectionnez Device Settings (Paramètres du dispositif) > Local Port Configuration (Configuration du port local). La page des paramètres du port local s'ouvre.
2. Cochez la case en regard d'Enable Standard Local Port (Activer le port local standard) pour l'activer. Désélectionnez la case à cocher pour le désactiver. Par défaut, le port local standard est activé, mais peut être désactivé selon les besoins. Le navigateur redémarrera lorsque cette modification sera effectuée. Si vous utilisez la fonction multiniveau, cette fonction sera désactivée car les deux ne peuvent pas être utilisées simultanément.
3. Si vous utilisez la fonction multiniveau, cochez la case Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local) et entrez le mot secret dans le champ Tier Secret (Secret du niveau). Pour paramétrer la fonction multiniveau, vous devez également configurer le dispositif de base sur la page Device Services (Services du dispositif). Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.
4. Le cas échéant, configurez les paramètres Local Port Scan Mode (Mode de balayage du port local). Ces paramètres s'appliquent à la fonction Scan Settings (Paramètres de balayage) accessible depuis la page Port. Reportez-vous à ***Balayage des ports*** (à la page 50).
   - Dans le champ Display Interval (10-255 sec) (Intervalle d'affichage (10 à 255 s), indiquez le nombre de secondes pendant lesquelles la cible sélectionnée doit rester affichée au centre de la fenêtre Port Scan (Balayage des ports).
   - Dans le champ Interval Between Ports (10 - 255 sec) (Intervalle entre les ports (10 à 255 s), indiquez l'intervalle de pause que doit respecter le dispositif entre les ports.

5. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - US
   - US/International (Anglais Etats-Unis/international)
   - United Kingdom
   - Français (France)
   - Allemand (Allemagne)
   - Japonais (JIS)
   - Chinois simplifié
   - Chinois traditionnel
   - Dubeolsik Hangul (Coréen)
   - Allemand (Suisse)
   - Portugais (Portugal)
   - Norvégien (Norvège)
   - Suédois (Suède)
   - Danois (Danemark)
   - Belge (Belgique)

Remarque : l'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de LX.

Remarque : Si vous utilisez un clavier turc, vous devez vous connecter à un serveur cible via Active KVM Client (AKC). Il n'est pas pris en charge par les autres clients Raritan.

6. Sélectionnez le raccourci-clavier du port local. Le raccourci-clavier du port local vous permet de retourner à l'interface de la console locale de LX lorsque l'interface d'un serveur cible est affichée. Le paramètre par défaut est Double Click Scroll Lock (Double-clic sur Arrêt défil), mais vous pouvez également sélectionner n'importe quelle combinaison de touches dans la liste déroulante :

Raccourci-clavier :	Appuyez sur :
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption

Raccourci-clavier :	Appuyez sur :
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur Maj gauche	La touche Maj gauche deux fois sans interruption
Double-clic sur la touche Ctrl gauche	La touche Ctrl gauche deux fois sans interruption

7. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre. Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local. Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à Exemples de touches de connexion pour obtenir des exemples de séquences de touches de connexion.
8. Réglez Video Switching Delay (Délai de commutation écran) entre 0 et 5 secondes, le cas échéant. En général, la valeur 0 est utilisée à moins que vous n'ayez besoin de plus de temps (certains écrans nécessitent plus de temps pour commuter la vidéo).
9. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique :
   a. Cochez la case Power Save Mode (Mode d'économie d'alimentation).
   b. Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.
10. Sélectionnez la résolution de la console locale de LX dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
    - 800 x 600
    - 1024 x 768
    - 1280 x 1024
11. Sélectionnez le taux de rafraîchissement dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
    - 60 Hz
    - 75 Hz
12. Sélectionnez le type d'authentification d'utilisateur locale.
    - Local/LDAP/RADIUS. Il s'agit de l'option recommandée. Pour plus d'informations sur l'authentification, reportez-vous à ***Authentification à distance*** (à la page 37).

- Aucun. Aucun processus d'authentification n'a lieu pour l'accès à la console locale. Cette option est recommandée pour les environnements sécurisés uniquement.

13. Cliquez sur OK.

Modification du paramètre de langue de l'interface utilisateur par défaut

L'interface utilisateur de LX prend en charge les langues suivantes :

- Japonais
- Chinois simplifié
- Chinois traditionnel

Pour modifier la langue de l'interface utilisateur :

1. Sélectionnez Device Settings > Language (Paramètres du dispositif > Langue). La page Language Settings (Paramètres de langue) s'ouvre :
2. Dans la liste déroulante Language, sélectionnez la langue à appliquer à l'interface utilisateur.
3. Cliquez sur Apply (Appliquer). Cliquez sur Reset Defaults (Rétablir les valeurs par défaut) pour retourner à l'anglais.

Remarque : lorsque vous appliquez une nouvelle langue, l'aide en ligne apparaît dans la langue sélectionnée.

Chapitre 7 Gestion de la sécurité

Dans ce chapitre

Security Settings (Paramètres de sécurité)

A partir de la page **Security Settings**, spécifiez les limitations de connexion, le blocage des utilisateurs, les règles de mot de passe, ainsi que les paramètres de chiffrement et de partage.

Les certificats SSL Raritan sont utilisés pour des échanges de clés publiques et privées. Ils fournissent un niveau de sécurité supplémentaire. Les certificats de serveur Web Raritan sont auto-signés. Les certificats d'applet Java sont signés par VeriSign. Le chiffrement garantit la sécurité de vos informations en les protégeant contre l'interception frauduleuse. Ces certificats garantissent que l'entité est bien Raritan, Inc.

Pour configurer les paramètres de sécurité :

1. Sélectionnez Security > Security Settings (Sécurité > Paramètres de sécurité). La page Security Settings s'ouvre.
2. Mettez à jour les paramètres de ***limitations de connexion*** (à la page 159) en fonction de vos besoins.
3. Mettez à jour les paramètres de ***mots de passe sécurisés*** (à la page 161) en fonction de vos besoins.
4. Mettez à jour les paramètres de ***blocage des utilisateurs*** (à la page 162) en fonction de vos besoins.
5. Mettez à jour les paramètres de ***chiffrement & partage*** (voir "***Encryption & Share (Chiffrement et partage)***" à la page 164) en fonction de vos besoins.
6. Cliquez sur OK.

Pour rétablir les paramètres par défaut :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

Limitations de connexion

A l'aide des limitations de connexion, spécifiez les restrictions en matière de connexion unique, de vieillissement de mot de passe et de déconnexion des utilisateurs inactifs.

Limitation	Description
Enable Single Login Limitation (Activer la limitation de connexion unique)	Si vous sélectionnez cette option, seule une connexion par nom d'utilisateur est autorisée à n'importe quel moment. En revanche, si elle est désélectionnée, une combinaison nom d'utilisateur/mot de passe donnée peut être connectée au dispositif à partir de plusieurs postes de travail clients simultanément.
Enable Password Aging (Activer le vieillissement du mot de passe)	Si vous sélectionnez cette option, tous les utilisateurs sont obligés de modifier leur mot de passe régulièrement en fonction du nombre de jours spécifiés dans le champ Password Aging Interval (Intervalle de vieillissement du mot de passe). Ce champ est activé et obligatoire lorsque la case Enable Password Aging (Activer le

Limitation	Description
	vieillissement du mot de passe) est cochée. Entrez le nombre de jours après lequel une modification de mot de passe est requise. Le nombre par défaut est 60 jours.
Log off idle users, After (1-365 minutes) (Déconnecter les utilisateurs inactifs, Après)	Cochez la case Log off idle users pour déconnecter automatiquement les utilisateurs après le délai spécifié dans le champ After (1-365 minutes). En l'absence d'activité du clavier ou de la souris, toutes les sessions et toutes les ressources sont déconnectées. En revanche, si une session de support virtuel est en cours, elle n'expire pas. Le champ After (Après) permet de définir le délai (en minutes) après lequel un utilisateur inactif est déconnecté. Ce champ est activé lorsque l'option Log Out Idle Users (Déconnecter les utilisateurs inactifs) est sélectionnée. La valeur saisie dans le champ peut aller jusqu'à 365 minutes.

Login Limitations
Enable Single Login Limitation
Enable Password Aging
Password Aging Interval (days)
60
Log Out Idle Users
Idle Timeout (minutes)
30

Mots de passe sécurisés

Les mots de passe sécurisés fournissent une authentification locale du système accrue. Utilisez les mots de passe sécurisés pour spécifier le format des mots de passe locaux valides de LX, tel que la longueur minimum et maximum, les caractères obligatoires et la conservation de l'historique des mots de passe.

Les mots de passe sécurisés créés par les utilisateurs doivent compter un minimum de 8 caractères avec au moins un caractère alphabétique et un caractère non alphabétique (signe de ponctuation ou chiffre). De plus, les quatre premiers caractères du mot de passe et du nom d'utilisateur ne peuvent pas être identiques.

Si cette option est sélectionnée, les règles des mots de passe sécurisés sont appliquées. Les utilisateurs dont les mots de passe ne répondent pas aux critères de mot de passe sécurisé sont automatiquement invités à modifier leur mot de passe lors de la connexion suivante. Si l'option est désélectionnée, seule la validation du format standard est appliquée. Lorsqu'elle est sélectionnée, les champs suivants sont activés et obligatoires :

Champ	Description
Minimum length of strong password (Longueur minimale du mot de passe sécurisé)	Le mot de passe doit compter au moins 8 caractères. La valeur par défaut est 8, mais vous pouvez entrer jusqu'à 63 caractères.
Maximum length of strong password (Longueur maximale du mot de passe sécurisé)	La valeur par défaut est de 8 au minimum et de 16 au maximum.
Enforce at least one lower case character (Imposer au moins un caractère minuscule)	Lorsqu'elle est cochée, cette option impose au moins un caractère minuscule dans le mot de passe.
Enforce at least one upper case character (Imposer au moins un caractère majuscule)	Lorsqu'elle est cochée, cette option impose au moins un caractère majuscule dans le mot de passe.
Enforce at least one numeric character (Imposer au moins un caractère numérique)	Lorsqu'elle est cochée, cette option impose au moins un caractère numérique dans le mot de passe.
Enforce at least one printable special character (Imposer au moins un caractère spécial imprimable)	Lorsqu'elle est cochée, cette option impose au moins un caractère spécial (imprimable) dans le mot de passe.

Champ	Description
Number of restricted passwords based on history (Nombre de mots de passe restreints en fonction de l'historique)	Ce champ représente la profondeur de l'historique des mots de passe ; c'est-à-dire le nombre de mots de passe précédents ne pouvant pas être répétés. La plage va de 1 à 12, la valeur par défaut étant 5.

Strong Passwords

Enable Strong Passwords

Minimum length of strong password

8

Maximum length of strong password

16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history

5

Blocage des utilisateurs

Les options de blocage d'utilisateurs spécifient les critères selon lesquels les utilisateurs se voient refuser l'accès au système après un nombre spécifique d'échecs de connexion.

Les trois options s'excluent les unes les autres :

Option	Description
Disabled (Désactivé)	Il s'agit de l'option par défaut. Les utilisateurs ne sont pas bloqués quel que soit le nombre d'échecs d'authentification.

Option	Description
Timer Lockout (Période de verrouillage)	Les utilisateurs se voient refuser l'accès au système après avoir dépassé le nombre d'échecs de connexion autorisé. Lorsque cette option est sélectionnée, les champs suivants sont activés : ▪ Attempts (Tentatives) - Il s'agit du nombre d'échecs de connexion après lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 10, la valeur par défaut étant 3 tentatives. ▪ Lockout Time (Durée de verrouillage) - Il s'agit du laps de temps pendant lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 1 440 minutes, la valeur par défaut étant 5 minutes. *Remarque : les utilisateurs dotés du rôle Administrateur ne sont pas concernés par les paramètres de période de verrouillage.*
Deactivate User-ID (Désactiver l'ID de l'utilisateur)	Sélectionnée, cette option indique que l'utilisateur ne peut plus accéder au système après un nombre spécifique de tentatives de connexion échouées, défini dans le champ Failed Attempts (Tentatives échouées) : ▪ Failed Attempts (Tentatives échouées) - Il s'agit du nombre d'échecs de connexion après lequel l'ID de l'utilisateur est désactivé. Le champ est activé lorsque l'option Deactivate User-ID (Désactiver l'ID de l'utilisateur) est sélectionnée. Les valeurs autorisées sont comprises entre 1 et 10. Lorsque l'ID d'un utilisateur est désactivé suite à un nombre spécifique d'échecs de connexion, l'administrateur doit modifier le mot de passe de l'utilisateur et activer le compte de celui-ci en cochant la case Active (Actif) dans la page User (Utilisateur).

User Blocking

Disabled

Timer Lockout

Attempts

3

Lockout Time

5

Deactivate User-ID

Failed Attempts

3

Encryption & Share (Chiffrement et partage)

A l'aide des paramètres de chiffrement et de partage, vous pouvez spécifier le type de chiffrement utilisé, les modes de partage PC et VM, ainsi que le type de réinitialisation effectuée lorsque le bouton Reset de LX est enfoncé.

AVERTISSEMENT : si vous sélectionnez un mode de chiffrement non pris en charge par votre navigateur, vous ne pourrez pas utiliser ce dernier pour accéder à LX.

Pour configurer le chiffrement et le partage :

1. Sélectionnez une option dans la liste déroulante Encryption Mode (Mode de chiffrement). Lorsqu'un mode de chiffrement est sélectionné, un avertissement s'affiche si votre navigateur ne prend pas en charge ce mode. Dans ce cas, vous ne serez pas en mesure de vous connecter à LX. L'avertissement indique « When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the LX. » (Lorsque le mode de chiffrement est spécifié, assurez-vous que votre navigateur le prend en charge ; sinon, vous ne pourrez pas vous connecter à LX.).

Mode de chiffrement	Description
Auto	Il s'agit de l'option recommandée. LX négocie automatiquement au niveau le plus élevé de chiffrement possible.
RC4	Permet de sécuriser les noms d'utilisateur, les mots de passe et les

Raritan.

Mode de chiffrement	Description
	données KVM, notamment les transmissions vidéo, à l'aide de la méthode de chiffrement RSA RC4. Le protocole Secure Socket Layer (SSL) à 128 bits fournit un canal de communication privé entre le dispositif LX et l'ordinateur distant lors de l'authentification de la connexion initiale.
AES-128	La norme de chiffrement avancée (AES - Advanced Encryption Standard) est une norme approuvée par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) pour le chiffrement des données électroniques (la longueur de clé est de 128). Si l'option AES-128 est sélectionnée, assurez-vous que votre navigateur la prend en charge. Sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de la prise en charge du chiffrement AES par votre navigateur*** (à la page 167) pour plus d'informations.
AES-256	La norme de chiffrement avancée (AES - Advanced Encryption Standard) est une norme approuvée par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) pour le chiffrement des données électroniques (la longueur de clé est de 256). Si l'option AES-256 est sélectionnée, assurez-vous que votre navigateur la prend en charge. Sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de la prise en charge du chiffrement AES par votre navigateur*** (à la page 167) pour plus d'informations.

Remarque : MPC négocie systématiquement au niveau le plus élevé de chiffrement et s'adapte au mode de chiffrement paramétré s'il n'est pas défini sur Auto.

Remarque : si vous exécutez le système d'exploitation Windows XP® avec Service Pack 2, Internet Explorer® 7 ne peut pas se connecter à distance à LX à l'aide du chiffrement AES-128.

2. Apply Encryption Mode to KVM and Virtual Media (Appliquer le mode de chiffrement à KVM et aux supports virtuels). Lorsqu'elle est sélectionnée, cette option applique le mode de chiffrement sélectionné à la fois à KVM et aux supports virtuels. Après authentification, les données KVM et support virtuel sont également transférées avec un chiffrement de 128 bits.
3. PC share mode (Mode PC-Share). Détermine l'accès KVM à distance simultané global, permettant ainsi à huit utilisateurs distants au maximum de se connecter simultanément à une unité LX et d'afficher et gérer, en même temps, le même serveur cible par l'intermédiaire du dispositif. Cliquez sur la liste déroulante pour sélectionner une des options suivantes :
   - Private - No PC share (Privé - Pas de PC-Share). Il s'agit du mode par défaut. Seul un utilisateur à la fois peut accéder au serveur cible.
   - PC-Share - Huit utilisateurs maximum (administrateurs ou non) peuvent accéder simultanément aux serveurs cible KVM. Chaque utilisateur distant dispose du même contrôle au niveau du clavier et de la souris. Notez toutefois que le contrôle n'est pas homogène si un utilisateur n'arrête pas de taper ou de déplacer la souris.
4. En cas de besoin, sélectionnez VM Share Mode (Mode de partage du support virtuel). Cette option est activée uniquement si le mode PC-Share est activé. Lorsqu'elle est sélectionnée, cette option permet le partage des supports virtuels entre plusieurs utilisateurs ; cela signifie que de multiples utilisateurs peuvent accéder à la même session de supports virtuels. Par défaut, ce mode est désactivé.
5. Le cas échéant, sélectionnez Local Device Reset Mode (Mode Réinitialisation du dispositif local). Cette option spécifie les actions entreprises lorsque le bouton Reset (situé à l'arrière du dispositif) est enfoncé. Pour plus d'informations, reportez-vous à ***Réinitialisation de LX à l'aide du bouton de réinitialisation*** (à la page 209). Sélectionnez une des options suivantes :

Mode Réinitialisation du dispositif local	Description
Enable Local Factory Reset (Activer la réinitialisation locale des paramètres d'usine) (valeur par défaut).	Le dispositif LX retrouve les paramètres d'usine par défaut.

Mode Réinitialisation du dispositif local	Description
Enable Local Admin Password Reset (Activer la réinitialisation locale du mot de passe administrateur)	Permet de réinitialiser le mot de passe d'administrateur local uniquement. Le mot de passe raritan est rétabli.
Disable All Local Resets (Désactiver toutes les réinitialisations locales)	Aucune action de réinitialisation n'est entreprise.

Vérification de la prise en charge du chiffrement AES par votre navigateur

LX prend en charge AES-256. Pour savoir si votre navigateur utilise le chiffrement AES, vérifiez auprès de l'éditeur du navigateur ou consultez le site Web https://www.fortify.net/sslcheck.html à l'aide du navigateur avec la méthode de chiffrement que vous souhaitez vérifier. Ce site Web détecte la méthode de chiffrement de votre navigateur et fournit un rapport.

Remarque : Internet Explorer® 6 ne prend pas en charge le chiffrement AES 128 bits, ni le chiffrement AES 256 bits.

Chiffrement AES 256 bits : conditions préalables et configurations prises en charge

Le chiffrement AES 256 bits est pris en charge uniquement sur les navigateurs Web suivants :

- Firefox® 2.0.0.x et 3.0.x (et supérieur)
- Internet Explorer 7 et 8

Outre la prise en charge par le navigateur utilisé, le chiffrement AES 256 bits nécessite l'installation des fichiers Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy.

Selon la version de JRE™ utilisée, ces fichiers peuvent être téléchargés à la rubrique « other downloads » des pages suivantes dont voici les liens :

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp

Certificats SSL

LX utilise le protocole SSL (Secure Socket Layer) pour le trafic réseau chiffré entre lui-même et un client connecté. A l'établissement d'une connexion, LX doit s'identifier à un client à l'aide d'un certificat de cryptage.

Il est possible de générer une demande de signature de certificat (CSR) et d'installer un certificat signé par l'autorité de certification (CA) sur LX. L'autorité vérifie l'identité de l'auteur de la demande. Elle retourne alors un certificat contenant sa signature à l'auteur. Le certificat, portant la signature de l'autorité de certification reconnue, est utilisé pour confirmer l'identité du détenteur du certificat.

Remarque : la demande doit être générée sur LX.

Pour créer et installer un certificat SSL :

1. Sélectionnez Security (Sécurité) > SSL Certificate (Certificat SSL).
2. Remplissez les champs suivants :
   a. Common name (Nom courant) - Il s'agit du nom réseau de LX une fois qu'il est installé dans le réseau de l'utilisateur (en règle générale, le nom de domaine complet qualifié). Il est identique au nom utilisé pour accéder à LX avec un navigateur Web, mais sans le préfixe http://. Si le nom indiqué ici diffère du nom de réseau, le navigateur affiche un avertissement de sécurité lors de l'accès à LX par le biais du protocole HTTPS.
   b. Organizational unit (Unité organisationnelle) - Ce champ permet de spécifier le service, au sein d'une organisation, auquel LX appartient.
   c. Organization (Organisation) - Il s'agit du nom de l'organisation à laquelle LX appartient.
   d. Locality/City (Localité/Ville) - Il s'agit de la ville où se situe l'organisation.
   e. State/Province (Etat/Province) - Il s'agit de l'Etat ou de la province où se situe l'organisation.
   f. Country (ISO code) (Pays (code ISO)) - Il s'agit du pays où se situe l'organisation. Il s'agit du code ISO de deux lettres ; par exemple, DE pour l'Allemagne ou US pour les Etats-Unis.
   g. Challenge Password (Mot de passe challenge) - Certaines autorités de certification requièrent un mot de passe challenge pour autoriser des modifications ultérieures au certificat (par exemple, la révocation du certificat). La longueur minimale de ce mot de passe est de quatre caractères.

h. Confirm Challenge Password (Confirmer le mot de passe challenge) - Il s'agit de la confirmation du mot de passe challenge.

i. Email (Courriel) - Il s'agit de l'adresse électronique d'un contact responsable du dispositif LX et de sa sécurité.

j. Key length (Longueur de la clé) - Il s'agit de la longueur de la clé générée en bits. 1024 est la valeur par défaut.

k. Cochez la case Create a Self-Signed Certificate (Créer un certificat auto-signé) (le cas échéant).

3. Cliquez sur Create (Créer) pour générer la demande de signature de certificat (CSR).

Pour télécharger un certificat CSR :

1. La demande et le fichier contenant la clé privée utilisée lors de sa génération peuvent être téléchargés en cliquant sur Download.

Remarque : la demande de signature de certificat et le fichier de clé privée forment un ensemble et doivent être traités en conséquence. Si le certificat signé n'est pas associé à la clé privée utilisée pour le générer à l'origine, le certificat est inutile. Ceci s'applique au téléversement et au téléchargement de la demande de signature de certificat et de ses fichiers de clé privée.

2. Envoyez la demande enregistrée à une autorité de certification pour confirmation. Vous recevrez le nouveau certificat de l'autorité de certification.

Pour téléverser une demande CSR :

1. Téléversez le certificat dans LX en cliquant sur Upload.

Remarque : la demande de signature de certificat et le fichier de clé privée forment un ensemble et doivent être traités en conséquence. Si le certificat signé n'est pas associé à la clé privée utilisée pour le générer à l'origine, le certificat est inutile. Ceci s'applique au téléversement et au téléchargement de la demande de signature de certificat et de ses fichiers de clé privée.

Certificate Signing Request (CSR)

The following CSR is pending:

```
countryName              = US
stateOrProvinceName      = DC
localityName             = Washington
organizationName         = ACME Corp.
organizationalUnitName   = Marketing Dept.
commonName               = John Doe
emailAddress             = johndoe@acme.com
```

Download Delete

Certificate Upload

SSL Certificate File

Browse...

Upload

Une fois ces étapes effectuées, LX dispose de son propre certificat permettant d'identifier la carte auprès de ses clients.

Important : si vous détruisez la demande de signature de certificat sur LX, il n'existe aucun moyen de la récupérer ! Si vous l'avez supprimée par mégarde, vous devez répéter les trois étapes décrites ci-dessus. Pour éviter ceci, utilisez la fonction de téléchargement pour disposer d'une copie de la demande et de sa clé privée.

Chapitre 8 Maintenance

Dans ce chapitre

Journal d'audit

Un journal des événements du système LX est créé. Le journal d'audit peut contenir jusqu'à 2 Ko de données avant de commencer à écraser les entrées les plus anciennes. Pour éviter de perdre des données de journal d'audit, exportez-les sur un serveur syslog ou un gestionnaire SNMP. Configurez le serveur syslog ou le gestionnaire SNMP depuis la page Device Settings > Event Management (Paramètres du dispositif > Gestion des événements). Reportez-vous à ***Evénements capturés dans le journal d'audit et dans Syslog*** (à la page 231) pour plus d'informations sur ce qui est capturé dans le journal d'audit et dans syslog.

Pour consulter le journal d'audit de votre unité LX :

1. Sélectionnez Maintenance > Audit Log (Journal d'audit). La page Audit Log s'ouvre :

   La page du journal d'audit affiche les événements par date et heure (les événements les plus récents étant répertoriés en premier). Le journal d'audit fournit les informations suivantes :

   - Date : date et heure auxquelles l'événement s'est produit (système de 24 heures).
   - Event : nom de l'événement tel que répertorié dans la page Event Management (Gestion des événements).
   - Description : description détaillée de l'événement.

Pour enregistrer le journal d'audit :

Remarque : l'option d'enregistrement du journal d'audit est disponible uniquement sur la console distante de LX et non sur la console locale.

1. Cliquez sur Save to File (Enregistrer dans le fichier). Une boîte de dialogue Save File (Enregistrer le fichier) apparaît.

2. Choisissez le nom et l'emplacement du fichier, puis cliquez sur Save (Enregistrer). Le journal d'audit est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour naviguer dans le journal d'audit :

- Utilisez les liens [Older] (Plus ancien) et [Newer] (Plus récent).

Device Information (Informations sur le dispositif)

La page Device Information fournit des informations détaillées sur votre dispositif LX et sur les CIM en cours d'utilisation. Ces informations sont utiles si vous avez besoin de contacter l'assistance technique Raritan.

Pour afficher les informations sur votre LX et ses CIM :

- Sélectionnez Maintenance > Device Information (Informations sur le dispositif). La page des informations relatives au dispositif s'ouvre.

Les informations suivantes relatives à LX sont fournies :

- Modèle
- Numéro de version du matériel
- Version de firmware
- Numéro de série
- Adresse MAC

Les informations suivantes relatives aux CIM en cours d'utilisation sont fournies :

- (Numéro de) port
- Nom
- Type de CIM - DCIM ou VM
- Version de firmware
- Numéro de série du CIM - ce numéro provient directement des CIM pris en charge.

Remarque : seule la partie numérique ou les numéros de série sont affichés pour les CIM DCIM-USB, DCIM-PS2 et DCIM-USB G2. Par exemple, XXX1234567 est affiché. Le préfixe GN du numéro de série est affiché pour les CIM dotés d'un numéro de série configuré sur site.

Device Information

Model:	DLX-116
Hardware Revision:	0x10
Firmware Version:	2.4.5.1.79
Serial Number:	HKK1600002
MAC Address:	00:0d:5d:00:01:96

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
4	FC15	Dual-VM	3A88	GN000D5D01339E3C3D3F6D70666936
8	FC11	Dual-VM	3A88	PQ21010199
13	Dominion_LX_Port13	MCUTP	N/A	N/A
16	DominionLX	Dual-VM	3A88	PQ28450291

Backup and Restore (Sauvegarde et restauration)

La page Backup/Restore (Sauvegarder/Restaurer) vous permet de sauvegarder et de restaurer les paramètres et la configuration de votre LX.

Outre l'utilisation de la sauvegarde et de la restauration pour la continuité des opérations, vous pouvez utiliser cette fonction pour gagner du temps. Par exemple, vous pouvez donner rapidement un accès à votre équipe à partir d'un autre LX en sauvegardant les paramètres de configuration utilisateur du dispositif LX en cours d'utilisation et en restaurant ces paramètres sur le nouveau LX. Vous pouvez également configurer un LX et copier sa configuration dans plusieurs dispositifs LX.

Pour accéder à la page de sauvegarde/restauration :

- Sélectionnez Maintenance > Backup/Restore (Sauvegarder/Restaurer). La page Backup/Restore (Sauvegarder/Restaurer) s'ouvre.

Remarque : les sauvegardes sont toujours des sauvegardes complètes du système. Les restaurations, en revanche, peuvent être totales ou partielles selon votre sélection.

Pour effectuer une copie de sauvegarde de LX, si vous utilisez Firefox® ou Internet Explorer® 5 ou précédent :

1. Cliquez sur Backup (Sauvegarder). La boîte de dialogue File Download (Téléchargement de fichiers) s'ouvre.
2. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer sous) s'affiche.

3. Sélectionnez l'emplacement, spécifiez un nom de fichier, puis cliquez sur Save (Enregistrer). La boîte de dialogue Download Complete (Téléchargement terminé) s'affiche.
4. Cliquez sur Fermer. Le fichier de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour effectuer une copie de sauvegarde de LX, si vous utilisez Internet Explorer 6 ou supérieur :

1. Cliquez sur Backup (Sauvegarder). Une boîte de dialogue File Download (Téléchargement de fichier) contenant un bouton Open (Ouvrir) apparaît. Ne cliquez pas sur Open.

   Dans IE 6 (et supérieur), IE est utilisé comme application par défaut pour ouvrir les fichiers ; vous êtes donc invité à ouvrir le fichier au lieu de l'enregistrer. Pour éviter ce problème, vous devez remplacer l'application utilisée par défaut pour ouvrir les fichiers par WordPad®.

2. Pour ce faire :
   a. Enregistrez le fichier de sauvegarde. Le fichier de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.
   b. Une fois le fichier enregistré, localisez-le et cliquez dessus avec le bouton droit. Sélectionnez Propriétés.
   c. Dans l'onglet Général, cliquez sur Modifier et sélectionnez WordPad.

Pour restaurer votre LX :

AVERTISSEMENT : soyez prudent lorsque vous restaurez une version antérieure de votre LX. Les noms d'utilisateur et mots de passe spécifiés au moment de la sauvegarde sont restaurés. En cas d'oubli des anciens noms d'utilisateur et mots de passe administratifs, vous n'aurez plus accès à LX.

Par ailleurs, si vous utilisiez une adresse IP différente au moment de la sauvegarde, cette adresse IP est également restaurée. Si la configuration utilise DHCP, procédez à cette opération uniquement lorsque vous avez accès au port local pour vérifier l'adresse IP après la mise à jour.

1. Sélectionnez le type de restauration que vous souhaitez exécuter :
   - Full Restore (Restauration totale) - Restauration complète de l'intégralité du système. Généralement utilisée à des fins de sauvegarde et de restauration traditionnelles.

- Protected Restore (Restauration protégée) - Tout est restauré, hormis les informations spécifiques au dispositif : adresse IP, nom, etc. Cette option vous permet également de configurer un LX et de copier sa configuration dans plusieurs dispositifs LX.
- Custom Restore (Restauration personnalisée) - Avec cette option, vous pouvez sélectionner User and Group Restore (Restauration des utilisateurs et des groupes) et/ou Device Settings Restore (Restauration des paramètres du dispositif).
  - User and Group Restore (Restauration des utilisateurs et des groupes) - Cette option inclut uniquement les informations relatives aux utilisateurs et aux groupes. Cette option *ne restaure pas* le certificat et les fichiers de clé privée. Utilisez cette option pour configurer rapidement des utilisateurs sur un autre LX.
  - Device Settings Restore - Utilisez cette option pour copier rapidement les informations relatives au dispositif.

2. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
3. Localisez et sélectionnez le fichier de sauvegarde approprié puis cliquez sur Open (Ouvrir). Le fichier sélectionné apparaît dans le champ Restore File (Restaurer le fichier).
4. Cliquez sur Restore (Restaurer). La configuration (en fonction du type de restauration sélectionnée) est restaurée.

Mise à niveau des CIM

Utilisez cette procédure pour mettre à niveau les CIM à l'aide des versions de firmware stockées dans la mémoire de votre dispositif LX. En général, tous les CIM sont mis à niveau lorsque vous mettez à niveau le firmware du dispositif via la page Firmware Upgrade (Mise à niveau du firmware).

Remarque : seuls D2CIM-VUSB et D2CIM-DVUSB peuvent être mis à niveau à partir de cette page.

Pour mettre à niveau les CIM à l'aide de la mémoire de LX :

1. Sélectionnez Maintenance > CIM Firmware Upgrade (Mise à niveau du firmware du CIM). La page CIM Upgrade from (Mise à niveau du CIM à partir de) s'ouvre.

   Le (numéro de) port, le nom, le type, la version actuelle du CIM et la mise à niveau de la version du CIM sont affichés pour faciliter l'identification des CIM.
2. Cochez la case Selected (Sélectionné) pour chacun des CIM que vous voulez mettre à niveau.

3. Cliquez sur Upgrade (Mettre à niveau). Vous êtes invité à confirmer la mise à niveau.
4. Cliquez sur OK pour continuer la mise à niveau. Des barres de progression s'affichent lors de la mise à niveau. La mise à niveau prend environ 2 minutes (ou moins) par CIM.

Mise à niveau du firmware

La page Firmware Upgrade (Mise à niveau du firmware) permet de mettre à niveau le firmware de votre LX et de tous les CIM reliés. Cette page est disponible sur la console distante de LX uniquement.

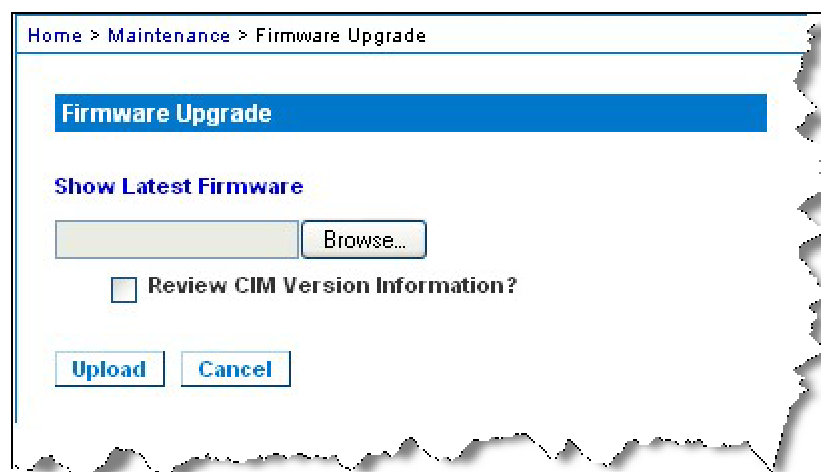
Important : ne mettez pas votre LX hors tension et ne déconnectez pas les CIM pendant la mise à niveau ; cela risque fortement d'endommager l'unité ou les CIM.

Pour mettre à niveau votre unité LX :

1. Localisez le fichier de distribution du firmware Raritan (*.RFP) sur la page des mises à niveau du firmware du ***site Web de Raritan http://www.raritan.com*** :
2. Décompressez le fichier. Lisez attentivement l'ensemble des instructions incluses dans les fichiers ZIP du firmware avant de procéder à la mise à niveau.

Remarque : copiez le fichier de mise à jour du firmware sur un PC local avant de procéder au téléversement. Ne chargez pas le fichier depuis un lecteur connecté en réseau.

3. Sélectionnez Maintenance > Firmware Upgrade (Mise à niveau du firmware). La page Firmware Upgrade (Mise à niveau du firmware) s'ouvre :



4. Cliquez sur Browse (Parcourir) pour accéder au répertoire où vous avez décompressé le fichier de mise à niveau.
5. Cochez la case Review CIM Version Information? (Vérifier les informations relatives à la version du CIM) pour afficher les informations relatives aux versions des CIM utilisés.
6. Cliquez sur Upload (Téléverser) dans la page de mise à niveau du firmware. Les informations concernant les numéros de mise à niveau et de version sont affichées pour votre confirmation (si vous avez opté pour la vérification des informations relatives au CIM, ces informations sont également affichées) :

   Remarque : à ce stade, les utilisateurs connectés sont déconnectés et toute nouvelle tentative de connexion est bloquée.

7. Cliquez sur Upgrade (Mettre à niveau). Patientez jusqu'à la fin de la mise à niveau. Des informations sur l'état et des barres de progression s'affichent pendant la mise à niveau. Une fois la mise à niveau terminée, l'unité redémarre (1 bip est émis pour signaler la fin du redémarrage).

A l'invite, fermez le navigateur et attendez environ 5 minutes avant de vous connecter de nouveau à LX.

Pour plus d'informations sur la mise à niveau du firmware du dispositif à l'aide de Multi-Platform Client, reportez-vous à **Mise à niveau du firmware du dispositif** dans le **manuel des clients d'accès KVM et série**.

Remarque : les mises à niveau de firmware ne sont pas prises en charge via modem.

Historique des mises à niveau

LX fournit des informations sur les mises à niveau effectuées sur LX et les CIM reliés.

Pour afficher l'historique des mises à niveau :

- Sélectionnez Maintenance > Upgrade History (Historique des mises à niveau). La page Upgrade History (Historique des mises à niveau) s'ouvre.

Les informations fournies concernent les mises à niveau de LX exécutées, l'état final de la mise à niveau, les heures de début et de fin, et les versions de firmware précédente et courante. Des informations relatives aux CIM sont également fournies ; pour les obtenir, cliquez sur le lien show (afficher) correspondant à une mise à niveau. Les informations relatives aux CIM fournies sont les suivantes :

- Type - Type du CIM.
- Port - Indique le port sur lequel est connecté le CIM.
- User - Indique l'utilisateur qui a effectué la mise à niveau.
- IP - Indiquez l'adresse IP de l'emplacement du firmware.
- Start Time - Indique l'heure de début de la mise à niveau.
- End Time - Indique l'heure de fin de la mise à niveau.
- Previous Version - Indique la version précédente du firmware de CIM.
- Upgrade Version - Indique la version courante du firmware de CIM.
- CIMs - Indique les CIM mis à niveau.
- Result - Résultat de la mise à niveau (réussite ou échec).

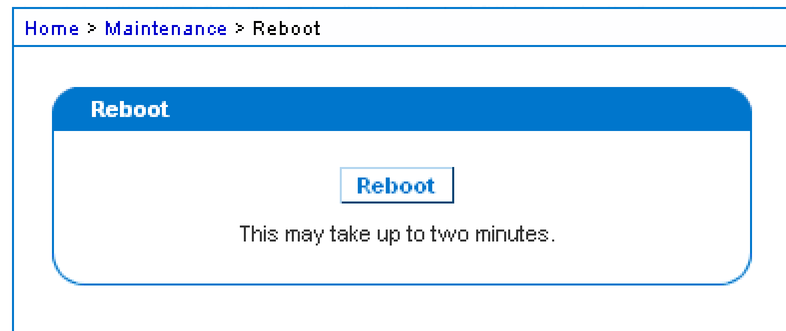
Redémarrage de LX

La page Reboot (Redémarrer) offre une manière sûre et contrôlée de redémarrer votre LX. Il s'agit de la méthode recommandée pour le redémarrage.

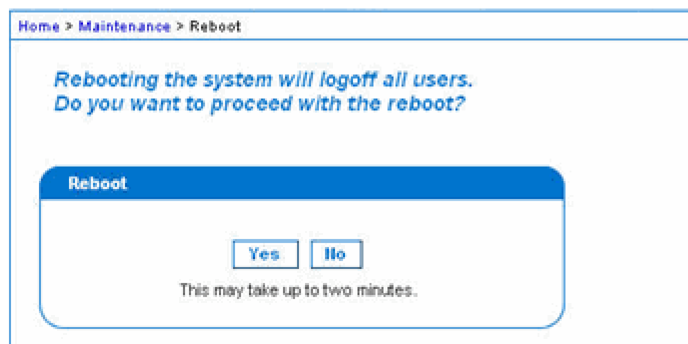
Important : toutes les connexions KVM et série sont fermées et tous les utilisateurs déconnectés.

Pour redémarrer votre LX :

1. Sélectionnez Maintenance > Reboot (Redémarrer). La page Reboot (Redémarrer) s'ouvre.



2. Cliquez sur Reboot. Vous êtes invité à confirmer l'action. Cliquez sur Yes (Oui) pour procéder au redémarrage.



Chapitre 9 Diagnostics

Dans ce chapitre

Page d'interface réseau

LX fournit des informations sur l'état de votre interface réseau.

Pour afficher les informations relatives à votre interface réseau :

- Sélectionnez Diagnostics > Network Interface (Interface réseau). La page d'interface réseau s'ouvre.

Les informations suivantes s'affichent :

- l'état de l'interface Ethernet (active ou non) ;
- si la commande ping peut être émise sur la passerelle ;
- le port LAN actif.

Pour actualiser ces informations :

- Cliquez sur Refresh (Actualiser).

Network Interface

Refresh

Result:

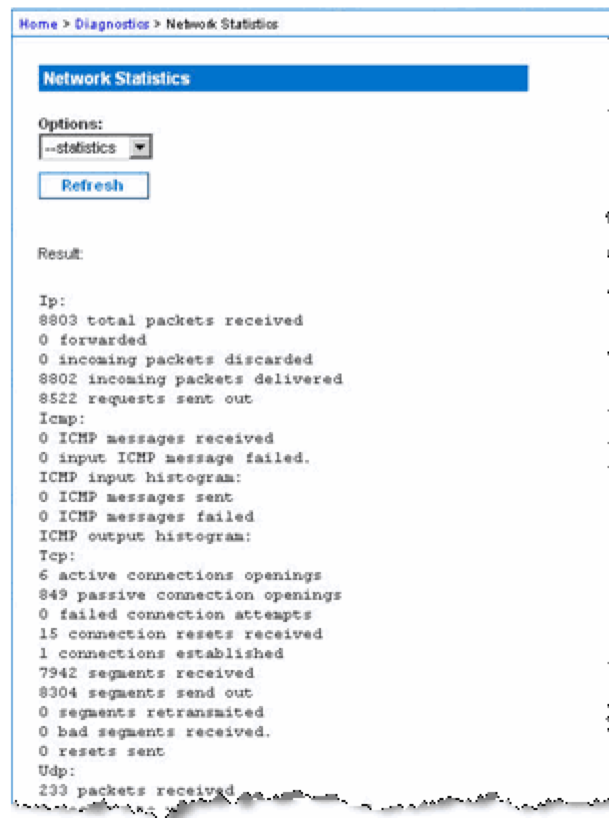
```
Link state: autonegotiation on, 100 Mbps, full duplex, link ok
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0d:5d:ca:b1:f8 brd ff:ff:ff:ff:ff:ff
inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
LAN 1 is active.
```

Page Network Statistics (Statistiques réseau)

LX fournit des statistiques sur votre interface réseau.

Pour afficher les statistiques relatives à votre interface réseau :

1. Sélectionnez Diagnostics > Network Statistics (Statistiques réseau). La page des statistiques réseau s'ouvre.
2. Sélectionnez l'option appropriée parmi celles de la liste déroulante Options :
   - Statistics - Génère une page similaire à celle affichée ici.



- Interfaces - Génère une page similaire à celle affichée ici.

Home > Diagnostics > Network Statistics

Network Statistics

Options:

--interfaces

Refresh

Result:

```
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1 1500 0 13828 0 0 0 8680 0 0 0 BMNRU
lo 16436 0 196 0 0 0 196 0 0 0 LRU
```

- Route - Génère une page similaire à celle affichée ici.

Home > Diagnostics > Network Statistics

Network Statistics

Options:

--route

Refresh

Result:

```
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.59.0 * 255.255.255.0 U 0 0 0 eth1
default 192.168.59.126 0.0.0.0 UG 0 0 0 eth1
```

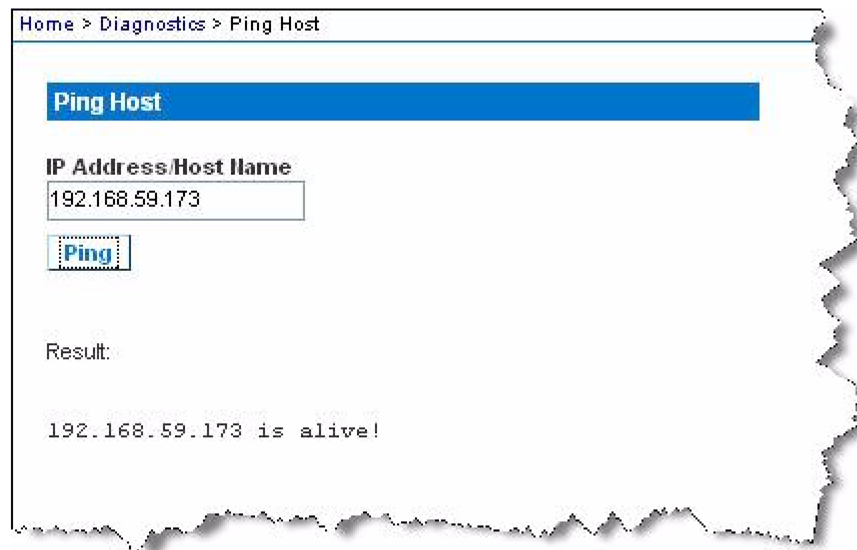
3. Cliquez sur Refresh (Actualiser). Les informations concernées sont affichées dans le champ Result (Résultat).

Page Ping Host (Envoi de commande Ping à l'hôte)

La commande Ping est un outil réseau qui permet de vérifier si un hôte ou une adresse IP spécifique est accessible via un réseau IP. Grâce à la page Ping Host (Envoyer une commande Ping à l'hôte), vous pouvez déterminer si un serveur cible ou un autre LX est accessible.

Pour envoyer une commande Ping à l'hôte :

1. Sélectionnez Diagnostics > Ping Host (Envoyer une commande Ping à l'hôte). La page Ping Host (Envoyer une commande Ping à l'hôte) apparaît.



2. Tapez le nom de l'hôte ou l'adresse IP dans le champ IP Address/Host Name.

Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Cliquez sur Ping. Les résultats de la commande Ping sont affichés dans le champ Result (Résultat).

Page Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte)

Cette page est un outil réseau permettant de tracer l'itinéraire emprunté jusqu'au nom d'hôte ou jusqu'à l'adresse IP fournis.

Pour déterminer l'itinéraire jusqu'à l'hôte :

1. Sélectionnez Diagnostics > Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte). La page Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte) s'ouvre.

2. Tapez l'adresse IP ou le nom de l'hôte dans le champ IP Address/Host Name.

Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Sélectionnez une valeur dans la liste déroulante Maximum Hops (Sauts maximum) (de 5 à 50 par incréments de 5).

4. Cliquez sur Trace Route. La commande de détermination d'itinéraire est exécutée pour le nom d'hôte ou l'adresse IP, et le nombre de sauts maximum donnés. Les données de détermination d'itinéraire sont affichées dans le champ Result (Résultat).

Home > Diagnostics > Trace Route to Host

Trace Route to Host

IP Address/Host Name

192.168.59.173

Maximum Hops:

10

Trace Route

Result:

traceroute started wait for 2mins....
traceroute to 192.168.59.173 (192.168.59.173), 10 hops max, 40 byte packets
1 192.168.59.173 (192.168.59.173) 0.497 ms 0.308 ms 0.323 ms

Page Device Diagnostics (Diagnostics du dispositif)

Remarque : cette page est en principe destinée aux techniciens de l'assistance. Vous pouvez l'utiliser lorsque l'assistance technique Raritan vous y invite directement.

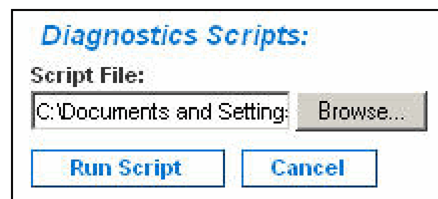
La page Device Diagnostics (Diagnostics du dispositif) télécharge les informations de diagnostic de LX vers l'ordinateur client. Deux opérations peuvent être effectuées sur cette page :

- Exécutez un script de diagnostics spécial fourni par le support technique Raritan lors d'une session de débogage d'erreurs critiques. Le script est téléversé sur le dispositif et exécuté. Une fois le script exécuté, vous pouvez télécharger les messages de diagnostics à l'aide de la fonction Save to File (Enregistrer dans le fichier).
- Téléchargez le journal de diagnostic du dispositif pour obtenir un instantané des messages de diagnostics de LX vers le client. Ce fichier chiffré est ensuite envoyé à l'assistance technique Raritan. Seul Raritan peut interpréter ce fichier.

Remarque : cette page n'est accessible qu'aux utilisateurs disposant de droits d'administration.

Pour exécuter les diagnostics du système LX :

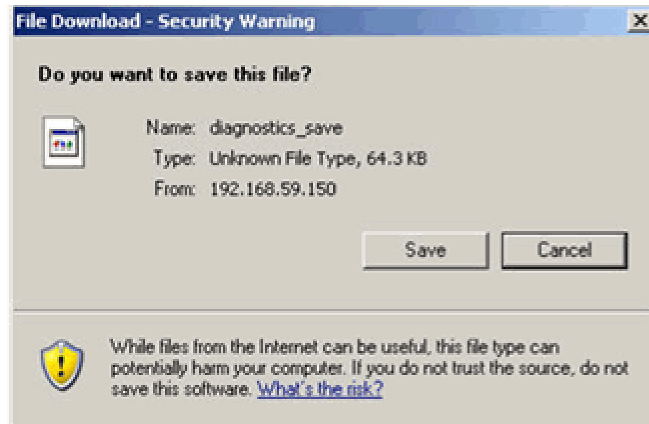
1. Sélectionnez Diagnostics > LX Diagnostics (Diagnostics de LX). La page de diagnostics de LX s'ouvre.
2. Pour exécuter un fichier de script de diagnostics qui vous a été envoyé par courrier électronique par l'assistance technique Raritan :
   a. Récupérez le fichier de diagnostics fourni par Raritan et décompressez-le si nécessaire.
   b. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
   c. Localisez et sélectionnez le fichier de diagnostics.
   d. Cliquez sur Open (Ouvrir). Le fichier s'affiche dans le champ Script File (Fichier de script).



   e. Cliquez sur Run Script (Exécuter le script). Envoyez ce fichier à l'assistance technique Raritan.

3. Pour créer un fichier de diagnostics à envoyer à l'assistance technique Raritan :

    a. Cliquez sur Save to File (Enregistrer dans le fichier). La boîte de dialogue File Download (Téléchargement de fichier) s'ouvre.



    b. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer sous) s'affiche.

    c. Localisez le répertoire voulu puis cliquez sur Save (Enregistrer).

    d. Envoyez ce fichier par courrier électronique à l'assistance technique Raritan.

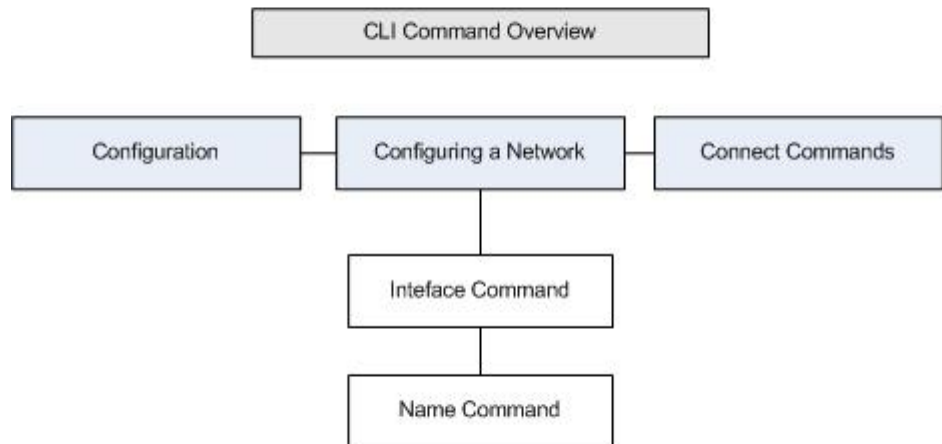
Chapitre 10 Interface de ligne de commande (CLI)

Dans ce chapitre

Présentation

L'interface de ligne de commande (CLI) permet de configurer l'interface réseau de LX et d'effectuer des fonctions de diagnostic si vous disposez des autorisations appropriées pour cela.

Les figures suivantes présentent les commandes CLI. Reportez-vous à ***Commandes CLI*** (à la page 193) pour consulter une liste de commandes, de définitions et de liens vers les sections de ce chapitre comportant des exemples de ces commandes.



Les commandes courantes suivantes peuvent être utilisées depuis tous les niveaux du CLI : top (haut), history (historique), log off (déconnecter), quit (quitter), show (afficher) et help (aide).

Accès à LX à l'aide de la CLI

Pour accéder à LX, choisissez l'une des méthodes suivantes :

- SSH via connexion IP

Un certain nombre de clients SSH sont disponibles et peuvent être obtenus sur les sites suivants :

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- SSH Client depuis ssh.com - ***www.ssh.com http://www.ssh.com***
- Applet SSH Client - ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

Connexion SSH à LX

Utilisez un client SSH prenant en charge SSHv2 pour effectuer la connexion à LX. Vous devez activer l'accès SSH dans la page Device Services (Services du dispositif).

Remarque : pour des raisons de sécurité, les connexions SSH V1 ne sont pas prises en charge par le dispositif LX.

Accès SSH depuis un PC Windows

Pour ouvrir une session SSH depuis un PC Windows® :

1. Lancez le logiciel client SSH.
2. Entrez l'adresse IP du serveur de LX. Par exemple, 192.168.0.192.
3. Choisissez SSH, qui utilise le port de configuration 22 par défaut.
4. Cliquez sur Open (Ouvrir).

L'invite `login as:` apparaît.

Reportez-vous à ***Connexion*** (à la page 190).

Accès SSH depuis un poste de travail UNIX/Linux

Pour ouvrir une session SSH depuis un poste de travail UNIX®/Linux® et vous connecter comme administrateur, entrez la commande suivante :

```
ssh -l admin 192.168.30.222
```

L'invite Password (Mot de passe) s'affiche.

Reportez-vous à ***Connexion*** (à la page 190).

Connexion

Pour vous connecter, entrez le nom d'utilisateur admin, comme indiqué ci-après :

1. Connectez-vous sous `admin`.
2. L'invite Password (Mot de passe) s'affiche. Entrez le mot de passe par défaut : *raritan*

   Le message de bienvenue s'affiche. Vous êtes maintenant connecté en tant qu'administrateur.

Après avoir pris connaissance de la section ***Navigation de la CLI*** (à la page 190), effectuez les tâches de configuration initiale.

Navigation de la CLI

Pour utiliser la CLI, il est essentiel d'en comprendre la navigation et la syntaxe. Certaines combinaisons de touches simplifient également l'utilisation de la CLI.

Saisie automatique des commandes

La CLI complète les commandes partiellement entrées. Entrez les premiers caractères d'une entrée et appuyez sur la touche Tab. Si les caractères forment une correspondance unique, la CLI complétera la saisie.

- Si aucune correspondance n'est trouvée, la CLI affiche les entrées valides pour ce niveau.
- S'il existe plusieurs correspondances, la CLI affiche toutes les entrées valides.

Entrez des caractères supplémentaires jusqu'à ce que l'entrée soit unique et appuyez sur la touche Tab pour compléter la saisie.

Syntaxe CLI - Conseils et raccourcis

Conseils

- Les commandes sont répertoriées par ordre alphabétique.
- Les commandes ne sont pas sensibles à la casse.
- Les noms de paramètre sont composés d'un seul mot, sans trait de soulignement.
- Les commandes sans arguments affichent par défaut les paramètres actuels de la commande.
- Si vous entrez un point d'interrogation (?) après une commande, l'aide correspondant à celle-ci s'affiche.
- Une ligne verticale (|) indique un choix parmi un ensemble de mots-clés ou d'arguments facultatifs ou obligatoires.

Raccourcis

- Appuyez sur la flèche Haut pour afficher la dernière entrée.
- Appuyez sur la touche Retour arrière pour supprimer le dernier caractère tapé.
- Utilisez Ctrl + C pour interrompre une commande ou l'annuler si vous avez saisi des paramètres erronés.
- Utilisez la touche Entrée pour exécuter la commande.
- Appuyez sur la touche Tab pour compléter automatiquement une commande. Par exemple, `Admin Port > Conf` Le système affiche ensuite l'invite `Admin Port > Config >`.

Commandes courantes pour tous les niveaux de la CLI

Les commandes disponibles à tous les niveaux du CLI sont indiquées ci-après. Ces commandes permettent également de parcourir la CLI.

Commandes	Description
top	Revient au niveau supérieur de la hiérarchie CLI, ou à l'invite username.
history	Affiche les 200 dernières commandes entrées par l'utilisateur dans la CLI de LX.
help	Affiche une présentation de la syntaxe CLI.
quit	Fait revenir l'utilisateur au niveau précédent.
logout	Déconnecte la session utilisateur.

Configuration initiale à l'aide de la CLI

Remarque : ces étapes, qui utilisent la CLI, sont facultatives car cette même configuration peut être effectuée via KVM. Reportez-vous à **Mise en route** *(à la page 13) pour plus d'informations.*

Les dispositifs LX sont livrés avec les paramètres usine par défaut. Lorsque vous mettez sous tension le dispositif et vous y connectez pour la première fois, vous devez définir les paramètres de base suivants, pour permettre un accès sécurisé au dispositif depuis le réseau :

1. Réinitialisez le mot de passe administrateur. Tous les dispositifs LX sont livrés avec le même mot de passe par défaut. Pour éviter toute intrusion, il est donc impératif de remplacer le mot de passe admin raritan par un mot de passe personnalisé pour les administrateurs qui assureront la gestion du dispositif LX.
2. Affectez l'adresse IP, le masque de sous-réseau et l'adresse IP de passerelle pour autoriser l'accès à distance.

Définition des paramètres

Pour définir les paramètres, vous devez être connecté avec des privilèges d'administration. Au niveau supérieur, vous verrez l'invite `Username>`, qui pour la configuration initiale est `admin`. Entrez la commande top pour retourner au niveau de menu supérieur.

Remarque : si vous êtes connecté sous un nom d'utilisateur différent, ce nom apparaîtra au lieu d'admin.

Définition des paramètres réseau

Les paramètres réseau sont configurés à l'aide de la commande d'interface.

```
Admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1
mode auto
```

Lorsque la commande est acceptée, le dispositif abandonne automatiquement la connexion. Vous devez vous reconnecter au dispositif à l'aide de la nouvelle adresse IP, et du nom d'utilisateur et du mot de passe que vous avez créés dans la section de réinitialisation de mot de passe usine par défaut.

Important : en cas d'oubli du mot de passe, LX doit être réinitialisé à la valeur par défaut usine à l'aide du bouton Reset à l'arrière de LX. Les tâches de configuration initiale doivent être alors exécutées à nouveau.

LX est maintenant doté d'une configuration de base et est accessible à distance via SSH, l'interface utilisateur ou localement à l'aide du port série local. L'administrateur doit configurer les utilisateurs et groupes, les services, la sécurité et les ports série par lesquels les cibles série sont connectées au LX.

Invites CLI

L'invite CLI indique le niveau de commande actuel. La partie racine de l'invite est le nom de connexion. Pour une connexion de port série admin directe avec une application d'émulation de terminal, Admin Port est la partie racine d'une commande.

```
admin >
```

Pour SSH, admin est la partie racine de la commande :

```
admin > config > network >
```

0

Commandes CLI

- Entrez `admin > help`.

Commande	Description
config	Passe au sous-menu config.
diagnostics	Passe au sous-menu diag.
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
listports	Répertorie les ports accessibles.
logout	Déconnecte de la session CLI actuelle.
top	Revient au menu racine.
userlist	Répertorie les sessions utilisateur actives.

- Entrez `admin > config > network`.

Commande	Description
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
interface	Définit/Extrait les paramètres réseau.
ipv6_interface	Définit/Extrait les paramètres réseau IPv6.
logout	Déconnecte de la session CLI actuelle.
name	Configuration du nom de dispositif.
quit	Revient au menu précédent.
stop	Revient au menu racine.

Problèmes de sécurité

Eléments à considérer en matière de sécurité pour les serveurs de console :

- Chiffrement le trafic des données envoyées entre la console de l'opérateur et le dispositif LX.
- Authentification et autorisation des utilisateurs.
- Profil de sécurité.

LX prend en charge chacun de ces éléments ; toutefois, ils doivent être configurés avant l'utilisation générale.

Administration des commandes de configuration du serveur de console de LX

Remarque : les commandes CLI sont les mêmes pour les sessions SSH et Port local.

La commande Network est accessible depuis le menu Configuration de LX.

Configuration du réseau

Les commandes du menu Network permettent de configurer l'adaptateur réseau de LX.

Commandes	Description
interface	Configure l'interface réseau du dispositif LX.
name	Configuration du nom du réseau.
ipv6	Définit/Extrait les paramètres réseau IPv6.

Commande interface

La commande interface permet de configurer l'interface réseau de LX. La syntaxe de la commande interface est la suivante :

```
interface [ipauto <none|dhcp>] [ip <ipaddress>]
[mask <subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> Adresse IP

mask <subnetmask> Masque de sous-réseau

gw <ipaddress> Adresse IP de passerelle

mode <mode> Set Ethernet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Exemple d'utilisation de la commande interface

La commande suivante activer l'interface numéro 1, définit l'adresse IP, le masque et les adresses de passerelle. Elle définit également le mode sur détection automatique.

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12
mode auto
```

Commande name

La commande name permet de configurer le nom de réseau. La syntaxe de la commande name est la suivante :

```
name [devicename <nomDispositif>] [hostname
<nomHôte>]
```

Configuration du nom de dispositif.

```
devicename <devicename>   Nom du dispositif

hostname   <hostname>     Nom d'hôte privilégié
(DHCP uniquement)
```

Exemple d'utilisation de la commande name

La commande suivante définit le nom de réseau :

```
Admin > Config > Network > name devicename My-KSX2
```

Commande IPv6

Utilisez IPv6_command pour définir des paramètres réseau IPv6 et extraire les paramètres IPv6 existants.

Chapitre 11 Console locale de LX

Dans ce chapitre

Présentation

LX fournit un accès et une administration sur le rack via son port local qui intègre une interface utilisateur graphique par navigateur pour commuter rapidement et aisément entre différents serveurs. La console locale de LX offre une connexion analogique directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur. La console locale de LX fournit les mêmes fonctionnalités d'administration que la console distante LX.

Utilisateurs simultanés

La console locale LX offre un chemin d'accès indépendant aux serveurs cible KVM connectés. L'utilisation de la console locale n'empêche pas les autres utilisateurs de se connecter en même temps sur le réseau. Même lorsque des utilisateurs sont connectés à distance à LX, vous pouvez toujours accéder à vos serveurs simultanément à partir du rack via la console locale.

Interface de la console locale de LX : Dispositifs LX

Lorsque vous êtes situé au niveau du rack du serveur, LX permet une gestion KVM standard via la console locale de LX. La console locale de LX offre une connexion (analogique) KVM directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur.

Les interfaces graphiques utilisateur de la console locale de LX et de la console distante de LX présentent de nombreuses ressemblances. Les éventuelles différences sont indiquées dans l'aide.

L'option Factory Reset (Rétablir les valeurs usine) est disponible sur la console locale de LX et non sur la console distante de LX.

Sécurité et authentification

Pour utiliser la console locale de LX, vous devez d'abord vous authentifier à l'aide d'un nom d'utilisateur et d'un mot de passe valides. LX dispose d'un schéma d'authentification et de sécurité entièrement intégré que votre accès passe par le réseau ou le port local. Dans ces deux cas, LX ne permet l'accès qu'aux serveurs pour lesquels un utilisateur dispose de permissions. Reportez-vous à ***Gestion des utilisateurs*** (à la page 108) pour plus d'informations sur la définition des paramètres d'accès et de sécurité des serveurs.

Si votre LX a été configuré pour des services d'authentification externe (LDAP/LDAPS, RADIUS ou Active Directory), les tentatives d'authentification au niveau de la console locale sont également authentifiées à l'aide du service d'authentification externe.

Remarque : vous pouvez également ne spécifier aucune authentification pour l'accès à la console locale ; cette option est recommandée uniquement dans les environnements sécurisés.

Pour utiliser la console locale de LX :

1. Branchez un clavier, une souris et un affichage vidéo sur les ports locaux situés à l'arrière de LX.
2. Démarrez LX L'interface de la console locale de LX s'affiche.

Résolutions vidéo prises en charge - Console locale

Assurez-vous que la résolution vidéo et le taux de rafraîchissement de chaque serveur cible sont pris en charge par l'unité LX, et que le signal est non entrelacé.

La console locale de LX offre les résolutions suivantes pour prendre en charge divers écrans :

- 800 x 600
- 1024 x 768
- 1280 x 1024

Chacune de ces résolutions prend en charge un taux de rafraîchissement de 60 Hz et 75 Hz.

La résolution vidéo et la longueur de câble sont des facteurs importants dans la réalisation de la synchronisation de la souris. Reportez-vous à ***Distance de connexion et résolution vidéo du serveur cible*** (à la page 226).

Page Port Access (affichage de serveur de la console locale)

Une fois que vous êtes connecté à la console locale de LX, la page d'accès aux ports s'ouvre. Elle répertorie tous les ports de LX, les serveurs cible KVM connectés ainsi que leur état et leur disponibilité.

Si vous utilisez une configuration multiniveau où un dispositif LX de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, vous pouvez afficher les dispositifs en niveau sur la page Port Access (Accès aux ports) en cliquant sur l'icône Expand Arrow ▶ (flèche de développement) à gauche du nom du dispositif en niveau. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.

▶ Pour utiliser la page Port Access :

1. Connectez-vous à la console locale.
2. Cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche.

   Les serveurs cible KVM sont triés initialement par numéro de port. Vous pouvez modifier l'affichage en effectuant le tri sur n'importe quelle colonne.

   - Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif LX.

- Port Name (Nom de port) - Nom du port de LX. Initialement, ce champ est défini sur Dominion-LX-Port# mais vous pouvez remplacer ce nom par un autre plus parlant. Lorsque vous cliquez sur un lien Port Name (Nom du port), le menu d'action des ports (Port Action Menu) s'affiche.

Remarque : n'utilisez pas d'apostrophe pour le nom de port (CIM).

- Type - Type de serveur ou CIM.
- Status (Statut) - Le statut des serveurs cible standard est activé ou désactivé.
- Availability (Disponibilité) - La disponibilité du serveur.

3. Cliquez sur le nom du port du serveur cible auquel vous souhaitez accéder. Le menu d'action des ports (Port Action Menu) apparaît. Reportez-vous à Port Action Menu (Menu d'action de ports) pour plus d'informations sur les options de menu disponibles.
4. Sélectionnez la commande souhaitée dans le menu d'action des ports.

Pour modifier l'ordre de tri et/ou afficher des ports supplémentaires sur la même page :

1. Cliquez sur l'en-tête de la colonne par laquelle vous souhaitez effectuer un tri. La liste des serveurs cible KVM est triée par cette colonne.
2. Dans Rows per Page (Lignes par page), entrez le nombre de ports à afficher sur la page et cliquez sur Set (Définir).

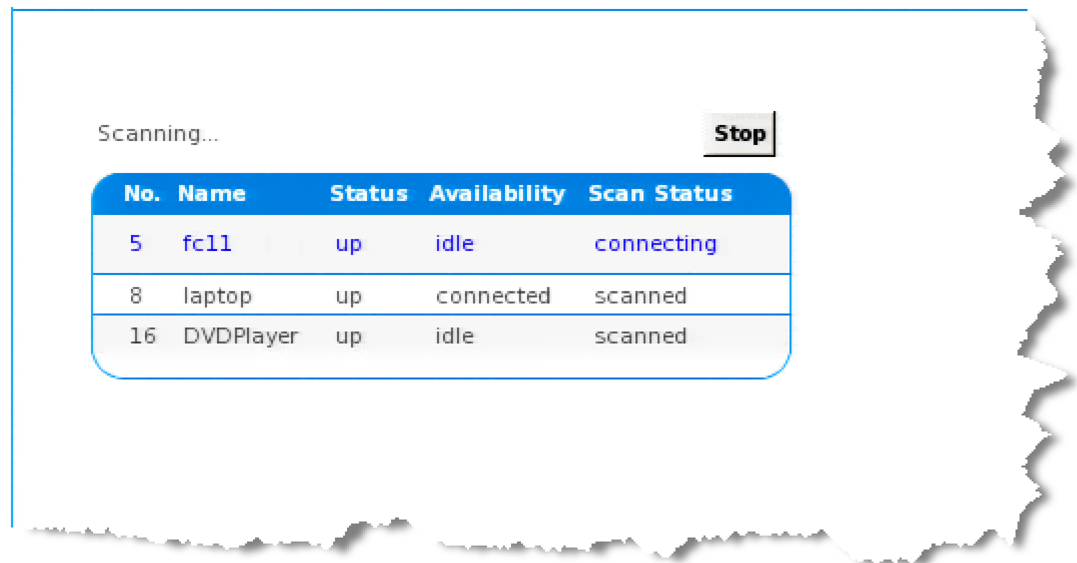
Accès à un serveur cible

Pour accéder à un serveur cible :

1. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu d'action des ports apparaît.
2. Sélectionnez Connect (Connecter) dans le menu d'action des ports. L'affichage vidéo bascule sur l'interface du serveur cible.

Balayage des ports - Console locale

La fonction de balayage de LX est prise en charge par la console locale. Les cibles détectées lors du balayage sont affichées dans la page Scan une par une, ce qui est différent du diaporama des ports de la console distante. Chaque cible est affichée sur la page pendant dix secondes par défaut, ce qui vous permet de la visualiser et de vous y connecter. Utilisez la séquence Local Port ConnectKey (Touche de connexion du port local) pour vous connecter à une cible lorsqu'elle est affichée et la séquence DisconnectKey (Touche de déconnexion) pour vous déconnecter.



Pour effectuer le balayage de cibles :

1. Depuis la console locale, cliquez sur l'onglet Set Scan (Balayage d'ensemble) dans la page Port Access (Accès aux ports).
2. Sélectionnez les cibles à inclure au balayage en cochant la case située à gauche de chacune, ou cochez la case au sommet de la colonne des cibles pour les sélectionner toutes.
3. Laissez la case Up Only (Activées seulement) cochée si vous ne souhaitez inclure au balayage que les cibles activées. Décochez-la pour inclure toutes les cibles, activées ou désactivées.
4. Cliquez sur Scan (Balayer) pour démarrer le balayage. Une fenêtre Port Scan (Balayage des ports) s'ouvre. Au fur et à mesure qu'une cible est détectée, elle est affichée dans la fenêtre.
5. Connectez-vous à une cible lorsqu'elle est affichée en utilisant la séquence ConnectKey.
6. Cliquez sur Stop Scan (Arrêter le balayage) pour arrêter le balayage.

Utilisation des options de balayage

Les options suivantes sont disponibles pour le balayage des cibles. A l'exception de l'icône Expand/Collapse (Développer/Réduire), toutes ces options sont sélectionnées à partir du menu Options en haut à gauche de l'afficheur Port Scan (Balayage des ports). Les valeurs par défaut des options sont rétablies lorsque vous fermez la fenêtre.

Masquer ou afficher les miniatures

- Utilisez l'icône Expand/Collapse (Développer/Réduire) en haut à gauche de la fenêtre pour masquer ou afficher les miniatures. Par défaut, la vue est développée.

Interrompre le diaporama des miniatures

- Pour interrompre la rotation des miniatures entre deux cibles, sélectionnez Options > Pause. La rotation des miniatures est le paramètre par défaut.

Reprendre le diaporama des miniatures

- Pour reprendre la rotation des miniatures, sélectionnez Options > Resume (Reprendre).

Dimensionner les miniatures dans l'afficheur Port Scan (Balayage des ports)

- Pour agrandir les miniatures, sélectionnez Options > Size (Taille) > 360x240.
- Pour réduire les miniatures, sélectionnez Options > Size (Taille) > 160x120. Il s'agit de la taille par défaut des miniatures.

Modifier l'orientation de l'afficheur Port Scan (Balayage des ports)

- Pour afficher les miniatures le long du bas de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Horizontal.
- Pour afficher les miniatures le long du côté droit de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Vertical. Il s'agit de la vue par défaut.

Raccourcis-clavier et touches de connexion

Comme l'interface de la console locale de LX est entièrement remplacée par l'interface du serveur cible auquel vous accédez, un raccourci-clavier est utilisé pour vous déconnecter d'une cible et retourner à l'interface utilisateur du port local. Une touche de connexion permet de se connecter à une cible ou de basculer entre plusieurs cibles.

Le raccourci-clavier du port local vous permet d'accéder rapidement à l'interface utilisateur de la console locale de LX lorsqu'un serveur cible est en cours d'affichage. L'opération définie par défaut est d'appuyer deux fois rapidement sur la touche Arrêt défil, mais vous pouvez aussi spécifier une autre combinaison de touches (reportez-vous à la page de paramétrage des ports locaux) comme raccourci-clavier. Reportez-vous à Configuration des paramètres de port local de la console locale de LX pour plus d'informations.

Exemples de touches de connexion

Serveurs standard	
Action de la touche de connexion	**Exemple de séquence de touches**
Accès à un port depuis l'interface utilisateur du port local	Accès au port 5 depuis l'interface utilisateur du port local : • Appuyez sur la touche Alt > Appuyez sur la touche 5 et relâchez-la > Relâchez la touche Alt
Permutation entre les ports	Passer du port cible 5 au port 11 : • Appuyez sur la touche Alt > Appuyez sur la touche 1 et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Relâchez la touche Alt
Déconnexion d'une cible et retour à l'interface utilisateur du port local	Se déconnecter du port cible 11 et retourner à l'interface utilisateur du port local (la page à partir de laquelle vous vous êtes connecté à la cible) : • Double-clic sur Arrêt défil

Combinaisons de touches Sun spéciales

Les combinaisons de touches suivantes pour les touches spéciales du serveur Sun™ Microsystems fonctionnent sur le port local. Ces touches spéciales sont disponibles dans le menu Clavier lorsque vous vous connectez à un serveur cible Sun :

Touche Sun	Combinaison de touches de port local
Again	Ctrl + Alt + F2
Props	Ctrl + Alt + F3
Undo	Ctrl + Alt + F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Muet	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	Aucune combinaison de touches
Alimentation	Aucune combinaison de touches

Retour à l'interface de la console locale de LX

Important : le raccourci-clavier par défaut de la console locale de LX consiste à appuyer deux fois sans interruption sur la touche Arrêt défil. Cette combinaison de touches peut être modifiée dans la page Local Port Settings (Paramètres du port local). Reportez-vous à Configuration des paramètres du port local de LX depuis la console locale.

Pour revenir à la console locale de LX à partir du serveur cible :

- Appuyez deux fois rapidement sur le raccourci-clavier (par défaut, la touche Arrêt défil). L'affichage écran passe de l'interface du serveur cible à celle de la console locale de LX.

Administration du port local

LX peut être géré par la console locale ou par la console distante. Notez que la console locale de LX donne également accès à :

- Factory Reset (Réinitialisation des paramètres d'usine)
- Paramètres du port local(disponible également dans la console distante)

Remarque : seuls les utilisateurs disposant des droits d'administrateur peuvent accéder à ces fonctions.

Configuration des paramètres du port local de la console locale de LX

A partir de la page de paramétrage du port local, vous avez la possibilité de personnaliser de nombreux paramètres de la console locale de LX, notamment le clavier, les raccourcis-clavier, le délai de commutation de l'écran, le mode d'économie d'alimentation, les paramètres de résolution de l'interface utilisateur locale et l'authentification d'utilisateur locale.

Remarque : seuls les utilisateurs disposant des droits d'administrateur peuvent accéder à ces fonctions.

Pour configurer les paramètres du port local :

Remarque : certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage doit se produire lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

1. Sélectionnez Device Settings (Paramètres du dispositif) > Local Port Configuration (Configuration du port local). La page des paramètres du port local s'ouvre.
2. Cochez la case en regard d'Enable Standard Local Port (Activer le port local standard) pour l'activer. Désélectionnez la case à cocher pour le désactiver. Par défaut, le port local standard est activé, mais peut être désactivé selon les besoins. Si vous utilisez la fonction multiniveau, cette fonction sera désactivée car les deux ne peuvent pas être utilisées simultanément.

3. Si vous utilisez la fonction multiniveau, cochez la case Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local) et entrez le mot secret dans le champ Tier Secret (Secret du niveau). Pour paramétrer la fonction multiniveau, vous devez également configurer le dispositif de base sur la page Device Services (Services du dispositif). Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 139) pour plus d'informations sur la fonction multiniveau.
4. Le cas échéant, configurez les paramètres Local Port Scan Mode (Mode de balayage du port local). Ces paramètres s'appliquent à la fonction Scan Settings (Paramètres de balayage) accessible depuis la page Port. Reportez-vous à ***Balayage des ports*** (à la page 50).
   - Dans le champ Display Interval (10-255 sec) (Intervalle d'affichage (10 à 255 s), indiquez le nombre de secondes pendant lesquelles la cible sélectionnée doit rester affichée au centre de la fenêtre Port Scan (Balayage des ports).
   - Dans le champ Interval Between Ports (10 - 255 sec) (Intervalle entre les ports (10 à 255 s), indiquez l'intervalle de pause que doit respecter le dispositif entre les ports.
5. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - US
   - US/International (Anglais Etats-Unis/international)
   - United Kingdom
   - Français (France)
   - Allemand (Allemagne)
   - Japonais (JIS)
   - Chinois simplifié
   - Chinois traditionnel
   - Dubeolsik Hangul (Coréen)
   - Allemand (Suisse)
   - Portugais (Portugal)
   - Norvégien (Norvège)
   - Suédois (Suède)
   - Danois (Danemark)
   - Belge (Belgique)

Remarque : l'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de LX.

Remarque : Si vous utilisez un clavier turc, vous devez vous connecter à un serveur cible via Active KVM Client (AKC). Il n'est pas pris en charge par les autres clients Raritan.

6. Sélectionnez le raccourci-clavier du port local. Le raccourci-clavier du port local vous permet de retourner à l'interface de la console locale de LX lorsque l'interface d'un serveur cible est affichée. Le paramètre par défaut est Double Click Scroll Lock (Double-clic sur Arrêt défil), mais vous pouvez également sélectionner n'importe quelle combinaison de touches dans la liste déroulante :

Raccourci-clavier :	**Appuyez sur :**
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur Maj gauche	La touche Maj gauche deux fois sans interruption
Double-clic sur la touche Ctrl gauche	La touche Ctrl gauche deux fois sans interruption

7. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre. Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local. Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à Exemples de touches de connexion pour obtenir des exemples de séquences de touches de connexion.
8. Cliquez sur OK.

Réinitialisation des paramètres d'usine de la console locale de LX

Remarque : cette fonction est disponible sur la console locale de LX uniquement.

LX offre plusieurs types de modes de réinitialisation à partir de l'interface utilisateur de la console locale.

Remarque : il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à ***Journal d'audit*** *(à la page 171).*

Pour procéder à une réinitialisation des paramètres d'usine :

1. Choisissez Maintenance > Factory Reset (Maintenance > Réinitialisation des paramètres usine). La page de réinitialisation des paramètres d'usine s'ouvre.
2. Choisissez l'option de réinitialisation appropriée parmi les suivantes :
   - Full Factory Reset (Réinitialisation intégrale des paramètres d'usine) : supprime la totalité de la configuration et rétablit complètement les paramètres d'usine du dispositif. Notez que toute association de gestion avec CommandCenter est interrompue. En raison du caractère intégral de cette réinitialisation, vous êtes invité à confirmer la réinitialisation des paramètres d'usine.
   - Network Parameter Reset (Réinitialisation des paramètres réseau) : rétablit les paramètres réseau du dispositif aux valeurs par défaut (cliquez sur Device Settings (Paramètres du dispositif) > Network Settings (Paramètres réseau) pour accéder à ces informations) :

- IP auto configuration (Configuration IP automatique)
- IP address (Adresse IP)
- Subnet mask (masque de sous-réseau)
- Gateway IP address (Adresse IP de passerelle)
- Primary DNS server IP address (Adresse IP du serveur DNS primaire)
- Adresse IP du serveur DNS secondaire (Adresse IP du serveur DNS secondaire)
- Discovery port (Port de détection)
- Bandwidth limit (Limite de bande passante)
- LAN interface speed & duplex (Vitesse & duplex de l'interface LAN).

3. Cliquez sur Reset (Réinitialiser) pour continuer. Vous êtes invité à confirmer la réinitialisation des paramètres d'usine car tous les paramètres réseau seront effacés définitivement.
4. Cliquez sur OK pour continuer. Quand vous avez terminé, le dispositif LX est automatiquement redémarré.

Réinitialisation de LX à l'aide du bouton de réinitialisation

Sur le panneau arrière du dispositif figure un bouton Reset (Réinitialiser). Il est encastré pour éviter les réinitialisations accidentelles (vous aurez besoin d'un objet pointu pour utiliser ce bouton).

Les opérations effectuées lorsque le bouton de réinitialisation est enfoncé sont définies dans l'interface utilisateur graphique. Reportez-vous à ***Encryption & Share (Chiffrement et partage)*** (à la page 164).

Remarque : il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à **Journal d'audit** *(à la page 171).*

Pour réinitialiser le dispositif :

1. Mettez LX hors tension.
2. Utilisez un objet pointu pour appuyer sur le bouton Reset (Réinitialiser) et pour le maintenir.
3. Tout en continuant à maintenir enfoncé le bouton Reset, mettez à nouveau sous tension le dispositif LX.

4. Continuez de maintenir le bouton enfoncé pendant 10 secondes. Une fois le dispositif réinitialisé, deux bips courts signalent la fin de l'opération.



Annexe A Spécifications

Dans ce chapitre

Spécifications de LX

Modèle Dominion LX	Description	Dimensions du produit (LxPxH), poids à l'expédition et alimentation	Environnement
DLX-108	Commutateur KVM	11.45" x 10,63 " x 1,73" ; 291 mm x 270 mm x 44 mm 8,82 lbs ; 4,0 kg Alimentation unique 100-240 V AC, 50-60 Hz, 0,5 A, 30 Watts, 25,794 kcal/h	Température d'exploitation : 0° – 40° C (32° – 104° F) Humidité : 20 % – 85 % HR

	sur IP à 8 ports extensible et économique, 1 utili		

	sateur distant, 1 utilisateur local, supports virtue		

	ls, alimentation et réseau local uniques		
DLX-116	Commutateu		

Raritan.

	r k V M s u r I P à 1 6 p o r t s e x t e n s i b l e e t é c o n o m i q u e , 1		

	utilisateur distant, 1 utilisateur local, supports		

	virtuels, alimentation et réseau local uniques			
DLX-216	Commu			

	tateur KVM sur IP à 16 ports extensible et économiq		

Raritan.

	ue, 2 utilisateurs distants, 1 utilisateur local, su		

	pports virtuels, alimentation et réseau local uniqu		

Raritan.

	e s
Matériel pris en charge	
Facteur de forme	Montage en rack 1U (supports de fixation fournis)
Port pour accès local	Vidéo : HD15(F) VGA ; Clavier/Souris : USB(F) ; 3 USB arrière
Exemples de résolutions vidéo	Mode texte PC : 640 x 350, 640 x 480, 720 x 400 Mode graphique PC : 640 x 480, 800 x 600, 1024 x 768, 1152 x 864, 1280 x 1024, 1440 x 900, 1680 x 1050,1600 x 1200, 1920 x 1080 Mode vidéo Sun : 1024 x 768, 1152 x 864, 1152 x 900, 1280 x 1024
Connexion à distance	
Ports	8 (DLX-108) ou 16 (DLX-116, DLX-216)
Utilisateurs	Utilisateur local ; 1 ou 2 utilisateurs distants (suivant le modèle)
Réseau	Accès Ethernet 10/100/1000 gigabits unique, double pile : IPv4 et IPv6
Protocoles	TCP/IP ; HTTP ; HTTPS ; UDP ; RADIUS ; SNMP ; DHCP ; PAP ; CHAP
Modules d'interface pour ordinateur (CIM) et câbles Cat5	
CIM Dominion	Disponibles pour USB, USB double, Universal Virtual Media/Absolute Mouse Synchronization, PS2, Sun, dispositifs série Dimensions (LxPxH) = 1,7" x 3,5" x 0,8" ; 43 mm x 90 mm x 19 mm (USB double) et 1,3" x 3,0" x 0,6" ; 33 mm x 76 mm x 15 mm (autres DCIM)
Câbles MCUTP Cat5	Câble KVM UTP pour PS/2, USB, Sun ; longueurs allant de 0,6 m (2 pieds) à 6 m (20 pieds). Spécifications : RJ45 <-> HDB-15M, mini-din 6 x 2 (PS/2), USB type A (USB/Sun)
Service et support	
Garantie*	Deux ans standard avec remplacement avancé

Voyants DEL

Témoins du panneau avant

- Démarrage - Témoins bleu et rouge = allumés
- Fonctionnel - Témoin bleu allumé
- Mise à niveau du firmware - Le témoin bleu clignote.

Témoins du panneau arrière

- 10 Mbps/Half - Les deux témoins clignotent.
- 10 Mbps/Full - Les deux témoins clignotent.
- 100 Mbps/Half - Le témoin jaune clignote.
- 1 Gbps/Full - Le témoin vert clignote.

Systèmes d'exploitation pris en charge (Clients)

Les systèmes d'exploitation suivants sont pris en charge sur Virtual KVM Client et Multi-Platform Client (MPC) :

Système d'exploitation client	Prise en charge des supports virtuels (VM) sur client ?
Windows 7®	Oui
Windows XP®	Oui
Windows 2008®	Oui
Windows Vista®	Oui
Windows 2000® SP4 Server	Oui
Windows 2003® Server	Oui
Windows 2008® Server	Oui
Red Hat® Desktop 5.0	Oui
Red Hat Desktop 4.0	Oui
Open SUSE 10, 11	Oui
Fedora® 13 et 14	Oui
Mac® OS	Oui
Solaris™	Non

Système d'exploitation client	Prise en charge des supports virtuels (VM) sur client ?
Linux®	Oui

Le plug-in JRE™ est disponible pour les systèmes d'exploitation Windows® 32 bits et 64 bits. MPC et VKC peuvent être lancés uniquement à partir d'un navigateur 32 bits, ou d'un navigateur 64 bits IE7 ou IE8.

Les prérequis des systèmes d'exploitation Windows Java™ 32 bits et 64 bits sont donnés ci-après.

Mode	Système d'exploitation	Navigateur
Windows x64 mode 32 bits	Windows XP®	• Internet Explorer® 6.0 SP1+ ou 7.0, IE 8 • Firefox® 1.06 - 3
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Firefox 1.06 - 3
	Windows Vista®	• Internet Explorer 7.0 ou 8.0
	Windows 7®	• Internet Explorer 9.0 • Firefox 1.06 - 3
Windows x64 mode 64 bits	Windows XP	SE 64 bits, navigateurs 32 bits : • Internet Explorer 6.0 SP1+, 7.0 ou 8.0 • Firefox 1.06 - 3 Mode 64 bits, navigateurs 64 bits : • Internet Explorer 7.0 ou 8.0
	Windows XP Professionnel®	
	Windows XP Edition Tablet PC®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

Navigateurs pris en charge

LX prend en charge les navigateurs suivants :

- Internet Explorer® 6 à 9
- Firefox® 1.5, 2.0, 3.0 (jusqu'à la version 3.6.17) et 4.0
- Safari® 3 ou supérieur

Modules CIM et systèmes d'exploitation pris en charge

Outre les modules D2CIM, la plupart des CIM Dominion sont pris en charge. Le tableau suivant indique les systèmes d'exploitation des serveurs cible, les CIM, les supports virtuels et les modes souris pris en charge.

Remarque : D2CIM-VUSB n'est pas pris en charge sur les cibles Sun™ (Solaris).

D2CIM LX pris en charge	Serveur cible et PDU de rack à distance (le cas échéant)	Support virtuel	Mode Souris absolue	Mode Souris intelligente	Mo So st
D2CIM-VUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora Core 3 et supérieur • Mac OS	✓	✓	✓	✓
	• Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5	✓		✓	✓
D2CIM-DVUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11	✓	✓	✓	✓

Raritan.

D2CIM LX pris en charge	Serveur cible et PDU de rack à distance (le cas échéant)	Support virtuel	Mode Souris absolue	Mode Souris intelligente	M So st
	• Fedora 8 - 11 • Mac OS				
	• Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5	✓		✓	✓

Résolutions vidéo prises en charge

Assurez-vous que la résolution vidéo et le taux de rafraîchissement de chaque serveur cible sont pris en charge par l'unité LX, et que le signal est non entrelacé.

La résolution vidéo et la longueur de câble sont des facteurs importants dans la réalisation de la synchronisation de la souris. Reportez-vous à ***Distance de connexion et résolution vidéo du serveur cible*** (à la page 226).

L'unité LX prend en charge ces résolutions :

Résolutions	
640 x 350 à 70Hz	1024 x768 à 85
640 x 350 à 85Hz	1024 x 768 à 75Hz
640 x 400 à 56Hz	1024 x 768 à 90Hz
640 x 400 à 84Hz	1024 x 768 à 100Hz
640 x 400 à 85Hz	1152 x 864 à 60Hz
640 x 480 à 60Hz	1152 x 864 à 70Hz
640 x 480 à 66,6Hz	1152 x 864 à 75Hz
640 x 480 à 72Hz	1152 x 864 à 85Hz
640 x 480 à 75Hz	1152 x 870 à 75,1Hz
640 x 480 à 85Hz	1152 x 900 à 66Hz
720 x 400 à 70Hz	1152 x 900 à 76Hz

Résolutions	
720 x 400 à 84Hz	1280 x 720 à 60Hz
720 x 400 à 85Hz	1280 x 960 à 60Hz
800 x 600 à 56Hz	1280 x 960 à 85Hz
800 x 600 à 60Hz	1280 x 1024 à 60Hz
800 x 600 à 70Hz	1280 x 1024 à 75Hz
800 x 600 à 72Hz	1280 x 1024 à 85Hz
800 x 600 à 75Hz	1360 x 768 à 60Hz
800 x 600 à 85Hz	1366 x 768 à 60Hz
800 x 600 à 90Hz	1368 x 768 à 60Hz
800 x 600 à 100Hz	1400 x 1050 à 60Hz
832 x 624 à 75,1Hz	1440 x 900 à 60Hz
1024 x 768 à 60Hz	1600 x 1200 à 60Hz
1024 x 768 à 70	1680 x 1050 à 60Hz
1024 x 768 à 72	1920 x 1080 à 60Hz

Distance de connexion et résolution vidéo du serveur cible

La distance maximale prise en charge dépend de plusieurs facteurs, notamment le type/la qualité du câble Cat5, le type et le fabricant du serveur, le pilote et l'écran vidéo, les conditions de l'environnement et les attentes de l'utilisateur. Pour les résolutions vidéo 1600 x 1200 et 1920 x 1080, le taux de rafraîchissement est de 60 et la distance maximum de connexion est de 15 mètres (50 pieds).

Remarque : en raison de la diversité des types et fabricants de serveurs, des versions de systèmes d'exploitation, des pilotes vidéo, etc. et de la nature subjective de la qualité vidéo, Raritan ne peut pas garantir les performances sur toutes les distances et dans tous les environnements.

Reportez-vous à ***Résolutions vidéo prises en charge*** (à la page 14) pour connaître les résolutions vidéo prises en charge par LX.

Modems certifiés

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

Connexion à distance

Connexion à distance	Détails
Réseau	Ethernet 10BASE-T, 100BASE-T et 1000BASE-T (Gigabit)
Protocoles	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Langues de clavier prises en charge

L'unité LX fournit un support clavier pour les langues indiquées dans le tableau suivant.

Remarque : vous pouvez utiliser le clavier pour le chinois, le japonais et le coréen à des fins d'affichage uniquement ; l'entrée de données dans la langue locale n'est pas prise en charge pour le moment en ce qui concerne les fonctions de la console locale de LX. Pour plus d'informations sur les claviers non US, reportez-vous à **Remarques d'informations** *(à la page 242).*

Remarque : Raritan recommande d'utiliser système-config-clavier pour modifier les langues si vous travaillez dans un environnement Linux.

Langue	Régions	Configuration du clavier
Anglais (Etats-Unis)	Etats-Unis d'Amérique et la plupart des pays anglophones : Canada, Australie et Nouvelle-Zélande, par exemple.	Clavier américain
Anglais international	Etats-Unis d'Amérique et la plupart des pays où l'anglais est utilisé : les Pays-Bas par exemple.	Clavier américain

Langue	Régions	Configuration du clavier
Anglais britannique	Royaume-Uni	Clavier britannique
Chinois traditionnel	Hong Kong R.A.S., République de Chine (Taïwan)	Chinois traditionnel
Chinois simplifié	République populaire de Chine (continentale)	Chinois simplifié
Coréen	Corée du Sud	Hangeul Dubeolsik
Japonais	Japon	Clavier JIS
Français	France	Clavier AZERTY français.
Allemand	Allemagne et Autriche	Clavier QWERTZ allemand
Français	Belgique	Belge
Norvégien	Norvège	Norvégien
Danois	Danemark	Danois
Suédois	Suède	Suédois
Hongrois	Hongrie	Hongrois
Slovène	Slovénie	Slovène
Italien	Italie	Italien
Espagnol	Espagne et la plupart des pays hispanophones	Espagnol
Portugais	Portugal	Portugais

Ports TCP et UDP utilisés

Port	Description
HTTP, Port 80	Ce port peut être configuré selon les besoins. Reportez-vous à ***Paramètres des ports HTTP et HTTPS*** (à la page 137). Toutes les requêtes reçues par LX via HTTP (port 80) sont automatiquement transmises à HTTPS pour garantir une sécurité complète. Pour plus de facilité, LX répond au port 80 (les utilisateurs n'ont ainsi pas à taper explicitement dans le champ URL pour accéder à LX) tout en préservant un niveau complet de sécurité.
HTTPS, Port 443	Ce port peut être configuré selon les besoins. Reportez-vous à ***Paramètres des ports HTTP et HTTPS*** (à la page 137). Par défaut, ce port est utilisé à diverses fins, notamment pour le serveur Web du client HTML, le téléchargement du logiciel client (MPC/VKC) sur l'hôte du client et le transfert de flux de données KVM et de support virtuel vers le client.
Protocole LX (Raritan KVM sur IP), Port 5000 configurable	Ce port est utilisé pour détecter d'autres dispositifs Dominion et pour la communication entre les dispositifs et les systèmes Raritan. Le port défini par défaut est le port 5000. Vous pouvez néanmoins configurer ce paramètre pour utiliser tout port TCP libre. Pour plus de détails sur la façon de configurer ce paramètre, reportez-vous à ***Paramètres réseau*** (à la page 132).
SNTP (serveur d'horloge) sur le port UDP configurable 123	LX offre la fonction facultative de synchroniser son horloge interne sur un serveur d'horloge central. Cette fonction nécessite l'utilisation du port UDP 123 (le port standard pour SNTP). Elle peut également être configurée sur le port de votre choix. **Facultatif**
LDAP/LDAPS sur les ports configurables 389 ou 636	Si LX est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole LDAP, les ports 386 ou 636 sont utilisés. Le système peut également être configuré pour utiliser le port de votre choix. **Facultatif**
RADIUS sur le port configurable 1812	Si LX est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole RADIUS, le port 1812 est utilisé. Le système peut également être configuré pour utiliser le port de votre choix. **Facultatif**
Gestion RADIUS sur le port configurable 1813	Si LX est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole RADIUS et qu'il utilise également Gestion RADIUS pour la consignation des événements, le port 1813 ou un port supplémentaire de votre choix est utilisé pour transmettre les notifications du journal.
SYSLOG sur le port UDP configurable 514	Si LX est configuré pour envoyer des messages à un serveur Syslog, les ports indiqués sont utilisés pour la communication (utilise le port UDP 514).
Ports UDP par	Le port 161 est utilisé pour l'accès SNMP entrant/sortant, en

défaut SNMP	lecture/écriture, et le port 162 est utilisé pour le trafic sortant des traps SNMP. **Facultatif**
Port TCP 21	Le port 21 est utilisé pour l'interface de ligne de commande de LX (lorsque vous travaillez avec l'assistance technique Raritan).

Evénements capturés dans le journal d'audit et dans Syslog

Vous trouverez ci-après la liste des événements capturés par le journal d'audit et syslog de LX :

- System Startup (Démarrage du système)
- System Shutdown (Arrêt du système)
- Network Parameter Changed (Paramètre réseau modifié)
- Port Status Changed (Statut du port modifié)
- Network Failure (Panne du réseau)
- Communication Error (Erreur de communication)
- Factory Reset (Réinitialisation des paramètres d'usine)
- Device Update Started (Mise à jour du dispositif démarrée)
- Device Update Completed (Mise à jour du dispositif terminée)
- Device Update Failed (Echec de la mise à jour du dispositif)
- Firmware Update Failed (Echec de la mise à jour du firmware)
- Firmware File Discarded (Fichier du firmware éliminé)
- Firmware Validation Failed (Echec de la validation du firmware)
- Configuration Backed Up (Configuration sauvegardée)
- Configuration Restored (Configuration restaurée)
- Port Connection Denied (Connexion du port refusée)
- Active USB Profile (Profil USB actif)
- Certficiate Update (Mise à jour de certificat)
- Date/Time Settings Changed (Paramètres de date/heure modifiés)
- Password Settings Changed (Paramètres de mot de passe modifiés)
- Login Failed (Echec de connexion)
- Password Changed (Mot de passe modifié)
- User Blocked (Utilisateurs bloqués)
- Port Connected (Port connecté)
- Port Disconnected (Port déconnecté)
- Access Login (Connexion d'accès)
- Access Logout (Déconnexion d'accès)
- Connection Lost (Connexion perdue)
- Session Timeout (Délai d'inactivité de session)
- VM Image Connected (Image VM connectée)
- VM Image Disconnected (Image VM déconnectée)
- CIM Update Started (Mise à jour du CIM démarrée)
- CIM Update Completed (Mise à jour du CIM terminée)

- CIM Connected (CIM connecté)
- CIM Disconnected (CIM déconnecté)
- Duplicate CIM Serial (Série CIM en double)
- Forced User Logout (Déconnexion forcée d'utilisateur)
- Scan Started (Balayage démarré)
- Scan Stopped (Balayage arrêté)
- User Added (Utilisateur ajouté)
- User Changed (Utilisateur modifié)
- User Deleted (Utilisateur supprimé)
- Group Added (Groupe ajouté)
- Group Changed (Groupe modifié)
- Group Deleted (Groupe supprimé)

Paramètres de vitesse réseau

Paramètre de vitesse réseau LX

Paramètre de port de commutateur réseau		**Auto**	**1000/Full**	**100/Full**	**100/Half**	**10/Full**	**10/Half**
	Auto	Vitesse disponible maximale	1000/Full	LX : 100/Full Commutateur : 100/Half	100/Half	LX : 10/Full Commutateur : 10/Half	10/Half
	1000/Full	1000/Full	1000/Full	Aucune communication	Aucune communication	Aucune communication	Aucune communication
	100/Full	LX : 100/Half Commutateur : 100/Full	LX : 100/Half Commutateur : 100/Full	100/Full	LX : 100/Half Commutateur : 100/Full	Aucune communication	Aucune communication
	100/Half	100/Half	100/Half	LX : 100/Full Commutateur : 100/Half	100/Half	Aucune communication	Aucune communication
	10/Full	LX : 10/Half Commutateur : 10/Full	Aucune communication	Aucune communication	Aucune communication	10/Full	LX : 10/Half Commutateur : 10/Full
	10/Half	10/Half	Aucune communication	Aucune communication	Aucune communication	LX : 10/Full Commutateur : 10/Half	10/Half

Légende :

(white box)	Ne fonctionne pas comme prévu
(green)	Pris en charge
(cyan)	Fonctionne ; non recommandé
(red)	NON pris en charge par la spécification Ethernet ; le produit peut communiquer mais des collisions se produisent.
(bold-bordered box)	Selon la spécification Ethernet, « aucune communication » ne devrait se produire ; notez toutefois que le comportement LX diffère du comportement attendu.

Remarque : pour assurer une communication réseau fiable, configurez LX et le commutateur LAN sur les mêmes valeurs de vitesse d'interface de réseau local et duplex. Par exemple, configurez LX et le commutateur LAN sur Autodetect (détection automatique) (recommandé) ou sur une vitesse fixe/duplex, comme 100Mo/s/Full.

Annexe B Mise à jour du schéma LDAP

Remarque : les procédures de ce chapitre ne doivent être effectuées que par des utilisateurs confirmés.

Dans ce chapitre

Renvoi des informations relatives aux groupes d'utilisateurs

Utilisez les informations de cette section pour renvoyer les informations relatives aux groupes d'utilisateurs (et faciliter le processus d'autorisation), une fois l'authentification réussie.

Depuis LDAP/LDAPS

Lorsqu'une demande d'authentification LDAP/LDAPS aboutit, >ProductName< détermine les autorisations accordées à un utilisateur donné selon les autorisations du groupe auquel il appartient. Votre serveur LDAP distant peut fournir ces noms de groupes d'utilisateurs en renvoyant un attribut désigné de la manière suivante :

rciusergroup attribute type: chaîne

Il est possible que cette opération nécessite une extension de schéma sur votre serveur LDAP/LDAPS. Consultez l'administrateur de votre serveur d'authentification pour activer cet attribut.

De plus, pour Microsoft® Active Directory®, le memberOf LDAP standard est utilisé.

A partir d'Active Directory (AD) de Microsoft

Remarque : seul un administrateur Active Directory® confirmé doit tenter cette opération.

Le renvoi des informations relatives aux groupes d'utilisateurs à partir de Microsoft® Active Directory pour le serveur du système d'exploitation Windows 2000® nécessite la mise à jour du schéma LDAP/LDAPS. Reportez-vous à la documentation Microsoft pour plus d'informations.

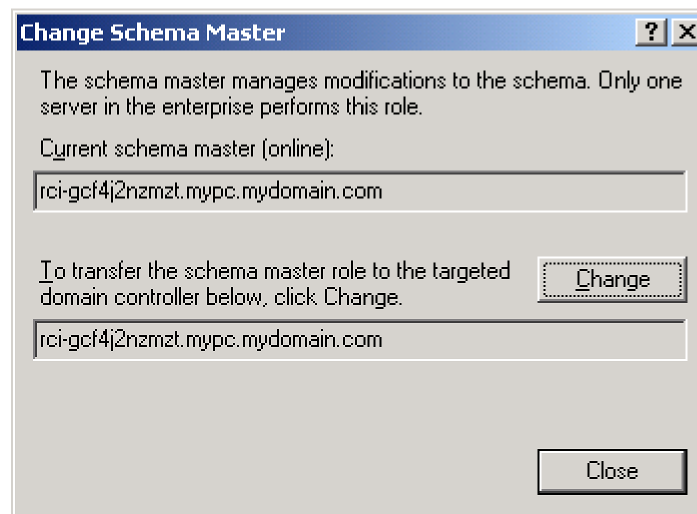
1. Installez le plug-in de schéma pour Active Directory. Reportez-vous à la documentation de Microsoft Active Directory pour obtenir des instructions.
2. Lancez la console Active Directory et sélectionnez Active Directory Schema (Schéma Active Directory).

Définition du Registre pour autoriser les opérations d'écriture sur le schéma

Pour autoriser un contrôleur de domaine à écrire sur le schéma, vous devez définir une entrée de Registre permettant les mises à jour du schéma.

Pour permettre les opérations d'écriture sur le schéma :

1. Cliquez avec le bouton droit de la souris sur le nœud racine Schéma Active Directory® dans le volet de gauche de la fenêtre, puis cliquez sur Maître d'opérations. La boîte de dialogue Changer le contrôleur de schéma s'affiche.



2. Cochez la case Le schéma peut être modifié sur ce contrôleur de domaine. **Facultatif**
3. Cliquez sur OK.

Création d'un attribut

Pour créer des attributs pour la classe rciusergroup :

1. Cliquez sur le symbole + en regard de Schéma Active Directory® dans le volet de gauche de la fenêtre.
2. Cliquez avec le bouton droit de la souris sur Attributs dans le volet de gauche.
3. Cliquez sur Nouveau, puis sélectionnez Attribut. Lorsque le message d'avertissement apparaît, cliquez sur Continuer ; la boîte de dialogue Créer un nouvel attribut s'affiche.

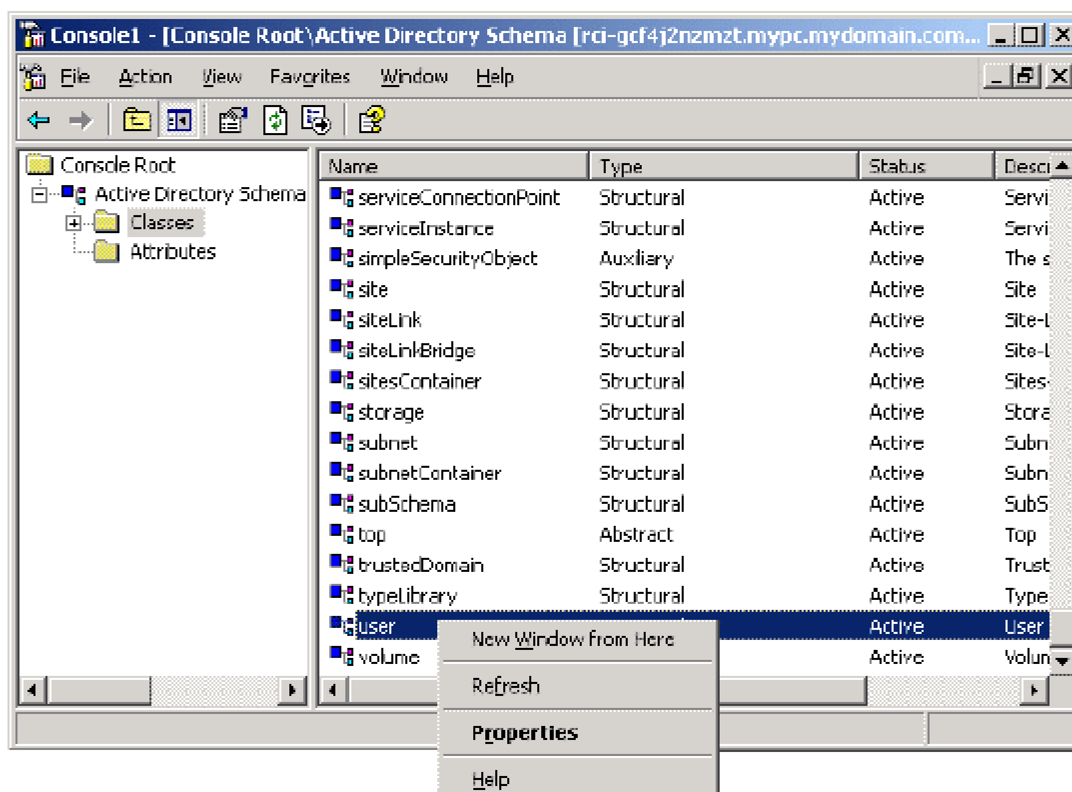
4. Tapez *rciusergroup* dans le champ Nom commun.
5. Tapez *rciusergroup* dans le champ Nom LDAP affiché.
6. Tapez *1.3.6.1.4.1.13742.50* dans le champ ID d'objet X.500 unique.
7. Entrez une description significative dans le champ Description.
8. Cliquez sur la flèche de la liste déroulante Syntaxe et sélectionnez Chaîne insensible à la casse dans la liste.
9. Tapez *1* dans le champ Minimum.
10. Tapez *24* dans le champ Maximum.

11. Cliquez sur OK pour créer l'attribut.

Ajout d'attributs à la classe

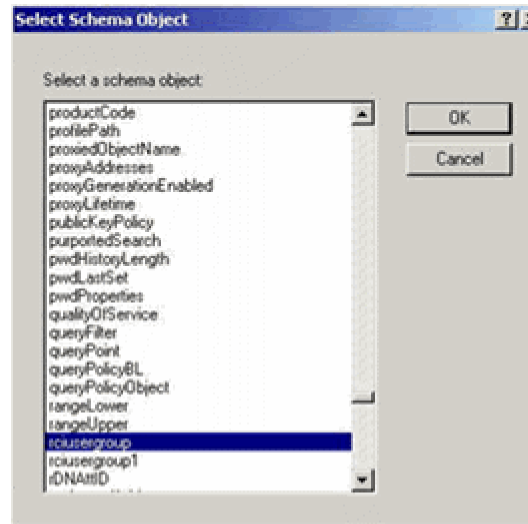
Pour ajouter des attributs à la classe :

1. Cliquez sur Classes dans le volet de gauche de la fenêtre.
2. Faites défiler le volet droit jusqu'à la classe user et cliquez dessus avec le bouton droit de la souris.



3. Sélectionnez Propriétés dans le menu. La fenêtre Propriétés de user s'affiche.
4. Cliquez sur l'onglet Attributs pour l'ouvrir.
5. Cliquez sur Add (Ajouter).

6. Sélectionnez rciusergroup dans la liste Sélectionnez l'objet Schéma.



7. Cliquez sur OK dans la boîte de dialogue Sélectionnez l'objet Schéma.

8. Cliquez sur OK dans la boîte de dialogue Propriétés de user.

Mise à jour du cache de schéma

Pour mettre à jour le cache du schéma :

1. Cliquez avec le bouton droit de la souris sur Schéma Active Directory® dans le volet de gauche de la fenêtre et sélectionnez Recharger le schéma.

2. Réduisez la console Active Directory Schema MMC (Microsoft® Management Console).

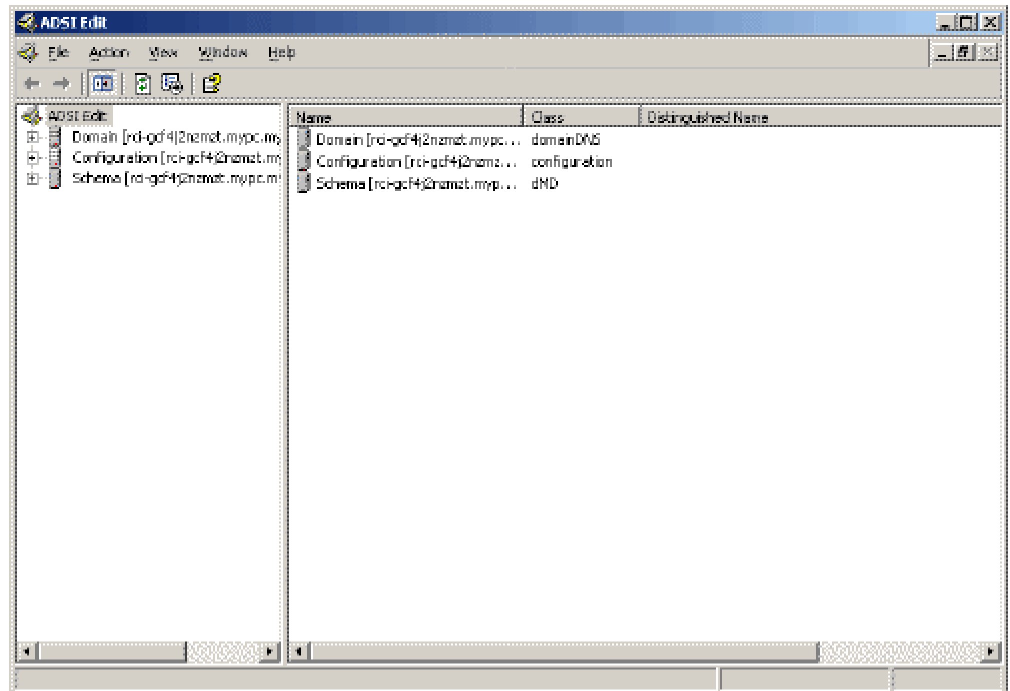
Modification des attributs rciusergroup pour les membres utilisateurs

Pour exécuter un script Active Directory® sur un serveur Windows 2003®, utilisez le script fourni par Microsoft® (disponible sur le CD d'installation de Windows Server 2003). Ces scripts sont chargés sur votre système lors de l'installation de Microsoft® Windows 2003. ADSI (ou Active Directory Service Interface) sert d'éditeur de bas niveau pour Active Directory. Il vous permet d'effectuer des tâches d'administration courantes, telles que l'ajout, la suppression et le déplacement d'objets avec un service d'annuaire.

Pour modifier les attributs d'un utilisateur individuel au sein du groupe rciusergroup, procédez comme suit :

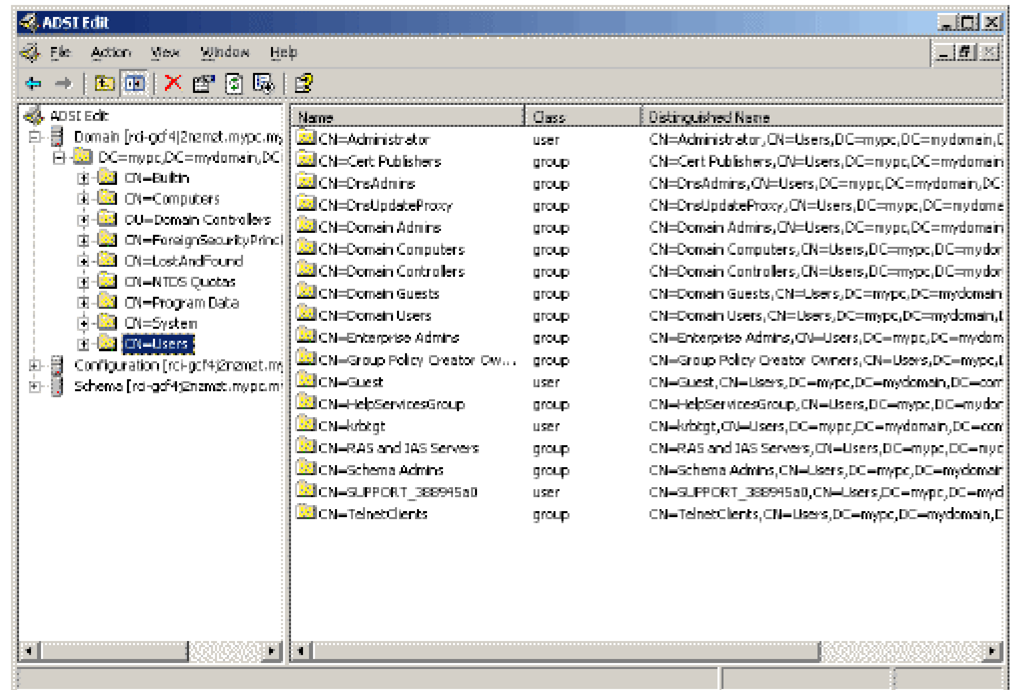
1. Sur le CD d'installation, sélectionnez Support > Tools (Outils).

2. Cliquez deux fois sur SUPTOOLS.MSI pour installer les outils de support.
3. Ouvrez le répertoire dans lequel les outils de support sont installés. Exécutez adsiedit.msc. La fenêtre Editeur ADSI s'ouvre.



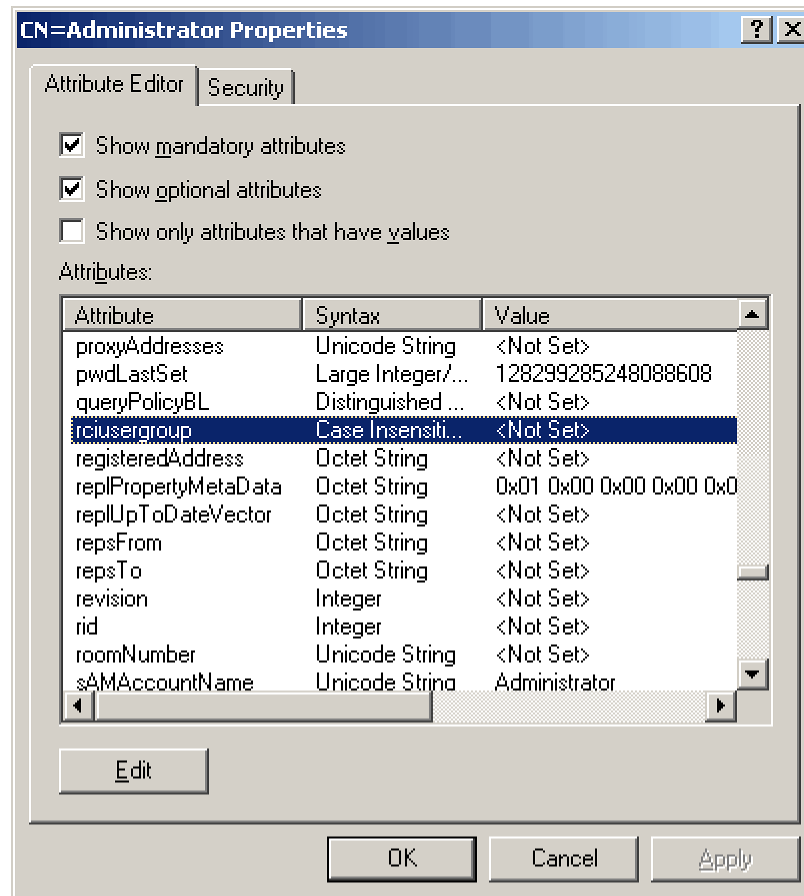
4. Ouvrez le domaine.

5. Dans le volet gauche de la fenêtre, sélectionnez le dossier CN=Users.

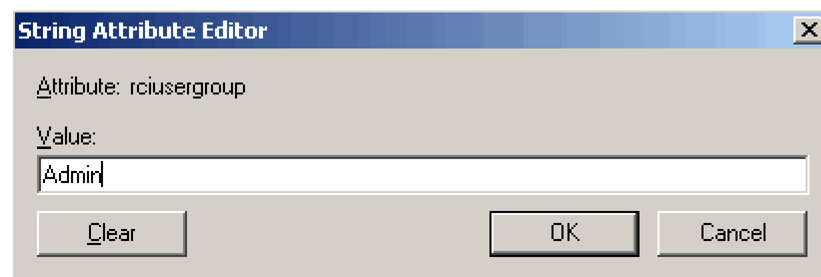


6. Recherchez le nom d'utilisateur dont vous souhaitez régler les propriétés dans le volet de droite. Cliquez avec le bouton droit sur le nom d'utilisateur et sélectionnez Propriétés.

7. Cliquez sur l'onglet Editeur d'attribut s'il n'est pas déjà ouvert. Sélectionnez rciusergroup dans la liste Attributs.



8. Cliquez sur Modifier. La boîte de dialogue Editeur d'attribut de chaîne apparaît.
9. Tapez le groupe d'utilisateurs (créé dans LX) dans le champ Modifier l'attribut. Cliquez sur OK.



Annexe C Remarques d'informations

Dans ce chapitre

Présentation

Cette section comporte des remarques importantes sur l'utilisation de LX. Les mises à jour à venir seront rapportées et disponibles en ligne via le lien d'aide de l'interface de la console distante de LX.

Remarque : Certaines rubriques de cette section traitent de plusieurs autres dispositifs Raritan car divers dispositifs sont concernés par ces informations.

Java Runtime Environment (JRE)

Important : il est recommandé de désactiver la mise en mémoire cache de Java™ et d'effacer la mémoire cache de celui-ci. Reportez-vous à la documentation Java ou au manuel des clients d'accès KVM et série pour plus d'informations.

La console locale de LX, KX II, KX II-101 et KX II-101-V2 et MPC requièrent Java Runtime Environment™ (JRE™) pour fonctionner car la console distante vérifie la version Java. Si la version est incorrecte ou obsolète, vous êtes invité à télécharger une version compatible.

Raritan vous recommande d'utiliser la version 1.6 de JRE pour garantir des performances optimales. La console distante et MPC fonctionnent cependant avec la version 1.6.x ou supérieure de ce programme, à l'exception de la version 1.6.2.

Remarque : pour que les claviers multilingues fonctionnent dans la console distante de LX, KX II, KX II-101 et KX II-101-V2 (Virtual KVM Client), installez la version multilingue de JRE.

Remarques sur la prise en charge d'IPv6

Java

Java™ 1.6 prend en charge IPv6 pour :

- Solaris™ 10 (et supérieur)
- Linux® kernel 2.1.2 (et supérieur)/RedHat 6.1 (et supérieur)

Java 5.0 et supérieur prend en charge IPv6 pour :

- Solaris 10 (et supérieur)
- Linux kernel 2.1.2 (et supérieur), kernel 2.4.0 (et supérieur) recommandés pour une meilleure prise en charge d'IPv6
- Systèmes d'exploitation Windows XP® SP1, Windows 2003® et Windows Vista®

Les configurations IPv6 suivantes *ne sont pas* prises en charge par Java :

- J2SE 1.4 ne prend pas en charge IPv6 sous Microsoft® Windows®.

Serveurs

- Linux kernel 2.4.0 ou supérieur est recommandé pour l'utilisation d'IPv6.
- Un noyau compatible IPv6 doit être installé ou le noyau doit être reconstruit avec les options IPv6 activées.
- Plusieurs utilitaires réseau doivent également être installés pour Linux si IPv6 est utilisé. Pour plus d'informations, reportez-vous à http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html

Serveurs

- Les utilisateurs de Windows XP et Windows 2003 doivent installer le service pack Microsoft IPV6 pour activer IPV6.

Mac Leopard

- IPv6 n'est pas pris en charge dans la version 2.0.20 de KX II pour Mac® Leopard®.

Samba

- IPv6 n'est pas pris en charge pour une utilisation avec les supports virtuels sous Samba.

Claviers

Claviers non américains

Clavier français

Caret (clients Linux® uniquement)

Virtual KVM Client et Multi-Platform Client (MPC) ne traitent pas la combinaison de touches Alt Gr + 9 comme le caret (^) lorsqu'un clavier français est utilisé avec des clients Linux.

► **Pour obtenir le caret :**

Sur un clavier français, appuyez sur la touche ^ (à droite de la touche P), puis immédiatement sur la barre d'espacement.

Ou, créez une macro constituée des commandes suivantes :

1. Appuyez sur la touche Alt Gr.
2. Appuyez sur la touche 9.
3. Relâchez la touche 9.
4. Relâchez la touche Alt Gr.

Remarque : ces procédures ne s'appliquent pas à l'accent circonflexe (au-dessus des voyelles). Dans tous les cas, la touche ^ (à droite de la touche P) fonctionne sur les claviers français pour créer l'accent circonflexe, lorsqu'elle est utilisée en combinaison avec un autre caractère.

Accent (clients Windows XP® seulement)

Depuis Virtual KVM Client et Multi-Platform Client, la combinaison de touches Alt Gr + 7 entraîne l'affichage en double du caractère accentué lors de l'utilisation d'un clavier français avec les clients Windows XP.

Remarque : ceci ne se produit pas avec les clients Linux.

Pavé numérique

Depuis Virtual KVM Client et Multi-Platform Client, les symboles du pavé numérique s'affichent comme suit lors de l'utilisation d'un clavier français :

Symbole du pavé numérique	Affiche
/	;

.	;

Tilde

Depuis Virtual KVM Client et Multi-Platform Client, la combinaison de touches Alt Gr + 2 ne produit pas le tilde (~) lors de l'utilisation d'un clavier français.

Pour obtenir le tilde :

Créez une macro constituée des commandes suivantes :

- Appuyez sur la touche Alt Gr.
- Appuyez sur la touche 2.
- Relâchez la touche 2.
- Relâchez la touche Alt Gr.

Préférence de la langue du clavier (clients Fedora Linux)

Etant donné que Sun™ JRE™ sous Linux® a des difficultés à générer les événements KeyEvents corrects pour les claviers dans d'autres langues configurés à l'aide des préférences système, Raritan recommande de configurer ces claviers à l'aide des méthodes décrites dans le tableau suivant.

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Anglais britannique	Paramètres système (centre de contrôle)
Français	Indicateur de clavier
Allemand	Indicateur de clavier
Hongrois	Paramètres système (centre de contrôle)
Espagnol	Paramètres système (centre de contrôle)
Allemand (Suisse)	Paramètres système (centre de contrôle)
Norvégien	Indicateur de clavier
Suédois	Indicateur de clavier
Danois	Indicateur de clavier
Japonais	Paramètres système (centre de contrôle)
Coréen	Paramètres système (centre de contrôle)
Slovène	Paramètres système (centre de contrôle)
Italien	Paramètres système (centre de contrôle)

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Portugais	Paramètres système (centre de contrôle)

Remarque : l'indicateur de clavier doit être utilisé sur les systèmes Linux utilisant l'environnement de bureau Gnome.

Sur un clavier hongrois depuis un client Linux, les lettres U et O avec deux accents aigus ne fonctionnent qu'avec JRE 1.6.

Plusieurs méthodes permettent de définir les préférences de langue de clavier sur les clients Fedora® Linux. La méthode suivante est obligatoire pour le mappage correct des touches des Virtual KVM Client et Multi-Platform Client (MPC).

Pour définir la langue du clavier à l'aide des paramètres système :

1. Depuis la barre d'outils, choisissez Système > Préférences > Clavier.
2. Ouvrez l'onglet Agencements.
3. Ajoutez ou sélectionnez la langue appropriée.
4. Cliquez sur Fermer.

Pour définir la langue du clavier à l'aide de l'indicateur de clavier :

1. Cliquez avec le bouton droit sur la barre de tâches et choisissez Ajouter au tableau de bord.
2. Dans la boîte de dialogue Ajouter au tableau de bord, cliquez avec le bouton sur Indicateur de clavier, et dans le menu, choisissez Ouvrir les préférences clavier.
3. Dans la boîte de dialogue Préférences clavier, cliquez sur l'onglet Agencements.
4. Ajoutez et enlevez des langues selon les besoins.

Clavier Macintosh

Lorsqu'un Macintosh® est utilisé comme client, les touches suivantes du clavier ne sont pas capturées par Java™ Runtime Environment (JRE™) :

- F9
- F10
- F11
- F14
- F15
- Monter le volume
- Descendre le volume
- Muet
- Ejection

En conséquence, Virtual KVM Client et Multi-Platform Client (MPC) ne sont pas en mesure de traiter ces touches d'un clavier de client Mac.

Fedora

Résolution du focus de Fedora Core

Lors de l'utilisation de Multi-Platform Client (MPC), il est parfois impossible de se connecter à un dispositif LX, KX II ou KSX II, ou d'accéder aux serveurs cible KVM (Windows®, SUSE, etc.). En outre, la combinaison de touches Ctrl+Alt+M n'affiche peut-être pas le menu des raccourcis-clavier. Cette situation se produit avec la configuration client suivante : Fedora® Core 6 et Firefox® 1.5 ou 2.0.

Des tests ont permis de déterminer que l'installation de libXp résolvait les problèmes de focus de fenêtre avec Fedora Core 6. Raritan a effectué les tests avec libXp-1.0.0.8.i386.rpm ; tous les problèmes de focus de clavier et de menus contextuels.

Remarque : libXp est également requis pour permettre le fonctionnement du navigateur SeaMonkey (précédemment Mozilla®) avec le plug-in Java™.

Synchronisation des pointeurs de souris (Fedora)

Lors d'une connexion en mode souris double à un serveur cible exécutant Fedora® 7, si les pointeurs des souris cible et locale perdent leur synchronisation, faire passer le mode de souris de ou vers Intelligent ou Standard peut améliorer la synchronisation. Le mode de souris unique peut également fournir un meilleur contrôle.

Pour resynchroniser les curseurs de souris :

- Utiliser l'option Synchronize Mouse (Synchroniser la souris) de Virtual KVM Client.

Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora

Si vous accédez à Firefox® et que vous utilisez un serveur Fedora®, Firefox risque de se bloquer à l'ouverture. Pour résoudre ce problème, installez le plug-in libnpjp2.so Java™ sur le serveur.

Modes et résolutions vidéo

Modes vidéo SUSE/VESA

L'outil de configuration SaX2 de SuSE X.org génère des modes vidéo à l'aide des entrées ModeLine du fichier de configuration X.org. Ces modes vidéo ne correspondent pas exactement au minutage du mode vidéo VESA (même si un écran VESA est sélectionné). LX, en revanche, s'appuie sur le minutage du monde VESA exact pour une synchronisation parfaite. Cette disparité peut entraîner des bordures noires, des sections d'image absentes et des parasites.

Pour configurer l'affichage vidéo SUSE :

1. Le fichier de configuration généré /etc/X11/xorg.conf inclut une section Monitor comportant une option appelée UseModes. Par exemple,
   UseModes "Modes[0]"
2. Mettez cette ligne en commentaire (à l'aide de #) ou supprimez-la complètement.
3. Redémarrez le serveur X.

Grâce à cette modification, le minutage du mode vidéo interne du serveur X sera utilisé et correspondra exactement au minutage du mode vidéo VESA, entraînant un affichage vidéo correct sur LX.

Résolutions vidéo prises en charge non affichées

Lorsque vous utilisez un CIM, certaines résolutions vidéo, indiquées dans Résolutions vidéo prises en charge, peuvent ne pas être disponibles à la sélection par défaut.

Pour afficher toutes les résolutions vidéo disponibles si elles n'apparaissent pas :

1. Branchez le moniteur.
2. Débranchez ensuite le moniteur et branchez le CIM. Toutes les résolutions vidéo sont à présent disponibles et peuvent être utilisées.

Ports USB VM-CIM et DL360

Les serveurs HP® DL360 sont dotés d'un port USB à l'arrière et d'un autre à l'avant. Avec DL360, les deux ports ne peuvent pas être utilisés simultanément. Aussi, un VM-CIM double ne peut pas être utilisé sur les serveurs DL360.

Toutefois, pour contourner ce problème, un concentrateur USB2 peut être connecté au port USB à l'arrière du dispositif et un VM-CIM double peut être connecté au concentrateur.

MCUTP

Le numéro de série et le nom du CIM fournis sur le MCUTP ne sont pas stockés dans le dispositif. Les ports MCUTP se comportent différemment des autres. Spécifiquement :

- Aucun stockage de nom sur le CIM ; le nom du port est un libellé associé au port tant que le type de ce dernier ne change pas en raison de la connexion d'un type de CIM différent.
- Des associations d'alimentation ne peuvent pas être effectuées sur des ports de ce type.
- Les paramètres de cible ne peuvent pas être appliqués aux ports de ce type.
- Le numéro de série apparaît sous la forme N/A sur les affichages indiquant le numéro de série du CIM ou dans les entrées de journal.
- Les ports de ce type ne peuvent pas être associés à des groupes de ports.
- Les ports de ce type ne peuvent pas être associés à des scripts de connexion.

Support virtuel

Utilisation du support virtuel via VKC et AKC dans un environnement Windows

Les droits Administrateur et utilisateur standard dans le système d'exploitation Windows XP® varient de ceux des systèmes d'exploitation Windows Vista® et Windows 7®.

Lorsqu'elle est activée dans Vista ou dans Windows 7, la fonction Contrôle d'accès d'utilisateur fournit le niveau de droits le plus bas dont un utilisateur a besoin pour une application. Par exemple, l'option Exécuter en tant qu'administrateur est fournie dans Internet Explorer® pour autoriser explicitement les utilisateurs à effectuer des tâches de niveau Administrateur, sinon celles-ci ne sont pas accessibles même si l'utilisateur dispose d'une connexion administrateur.

Ces deux fonctions affectent le type de supports virtuels accessibles aux utilisateurs via Virtual KVM Client (VKC) et Active KVM Client (AKC). Consultez l'aide Microsoft® pour en savoir plus sur ces fonctions et comment les utiliser.

La liste suivante répertorie des types de supports virtuels accessibles via VKC et AKC dans un environnement Windows. Ces fonctions sont classées par client, puis par rôle utilisateur Windows.

Windows XP

Si vous utilisez VKC et AKC dans un environnement Windows XP, les utilisateurs doivent disposer de droits Administrateur pour accéder à n'importe quel type de support virtuel autre que les connexions CD-ROM, les ISO et les images ISO.

Windows Vista et Windows 7

Si vous utilisez VKC et AKC dans un environnement Windows Vista ou Windows 7 et que la fonction Contrôle d'accès d'utilisateur est activée, les types de supports virtuels suivants sont accessibles suivant le rôle Windows de l'utilisateur :

Client	Administrateur	Utilisateur standard

Client	Administrateur	Utilisateur standard
AKC et VKC	Accès : • Lecteurs fixes et partitions de lecteurs fixes • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes	Accès : • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes

Partitions de lecteur

- Les limites en matière de partition de lecteur suivantes existent à travers les systèmes d'exploitation :
  - Les cibles Windows et Mac ne peuvent pas lire les partitions formatées Linux.
  - Windows® et Linux® ne peuvent pas lire les partitions formatées Mac.
  - Seules les partitions FAT Windows sont prises en charge par Linux.
  - FAT et NTFS Windows sont pris en charge par Mac.

  Les utilisateurs Mac doivent démonter les dispositifs déjà montés pour se connecter à un serveur cible. Utilisez >diskutil umount /dev/disk1s1 pour démonter le dispositif et diskutil mount /dev/disk1s1 pour le remonter.

Support virtuel non rafraîchi après l'ajout de fichiers

Après le montage d'un lecteur de support virtuel, si vous ajoutez des fichiers à ce lecteur, ces fichiers peuvent ne pas apparaître immédiatement sur le serveur cible. Supprimez, puis rétablissez la connexion de support virtuel.

Partitions système actives

Vous ne pouvez pas monter de partitions système actives à partir d'un client Mac ou Linux.

Les partitions de lecteur Ext3/4 Linux doivent être démontées à l'aide de umount /dev/<libellé de dispositif> avant d'établir une connexion au support virtuel.

Partitions de lecteur

Les limites en matière de partition de lecteur suivantes existent à travers les systèmes d'exploitation :

- Les cibles Windows et Mac ne peuvent pas lire les partitions formatées Linux.
- Windows® et Linux® ne peuvent pas lire les partitions formatées Mac.
- Seules les partitions FAT Windows sont prises en charge par Linux.
- FAT et NTFS Windows sont pris en charge par Mac.
- Les utilisateurs Mac doivent démonter les dispositifs déjà montés pour se connecter à un serveur cible. Utilisez >diskutil umount /dev/disk1s1 pour démonter le dispositif et diskutil mount /dev/disk1s1 pour le remonter.

Lecteur virtuel Linux répertorié deux fois

Pour les utilisateurs de KX II 2.4.0 (et supérieur) et de LX 2.4.5 (et supérieur) connectés aux clients Linux™ en tant qu'utilisateurs racine, les lecteurs sont répertoriés deux fois dans la liste déroulante Local Drive (Lecteur local). Vous verrez par exemple eg /dev/sdc et eg /dev/sdc1 où le premier lecteur est le secteur d'amorçage et le second, la première partition du disque.

Lecteurs mappés verrouillés Mac et Linux

Les lecteurs mappés à partir des clients Mac® et Linux® ne sont pas verrouillés lorsqu'ils sont montés sur des cibles connectées. Ceci ne concerne que KX II 2.4.0 (et supérieur) et LX 2.4.5 (et supérieur), qui offrent une prise en charge de Mac et de Linux.

Accès au support virtuel sur un serveur Windows 2000 utilisant un D2CIM-VUSB

Un lecteur local de support virtuel n'est pas accessible sur un serveur Windows 2000® utilisant un D2CIM-VUSB.

Durée d'amorçage du BIOS cible avec les supports virtuels

L'amorçage du BIOS de certaines cibles peut durer plus longtemps sur le support est monté virtuellement à la cible.

► Pour raccourcir la durée d'amorçage :

1. Fermez Virtual KVM Client pour libérer complètement les lecteurs de supports virtuels.

2. Redémarrez la cible.

Echec de connexion des supports virtuels lors de l'utilisation du haut débit

Dans certains cas, il peut être nécessaire de sélectionner l'option Use Full Speed for Virtual Media CIM (Utiliser le haut débit pour le CIM du support virtuel) lorsque la cible rencontre des difficultés avec la vitesse de connexion High Speed USB (USB à haut débit) ou qu'elle connaît des erreurs de protocole USB en raison d'une dégradation du signal due à la présence de connecteurs et de câbles supplémentaires..

CIM

Souris à 3 boutons Windows sur les cibles Linux

Lorsque vous utilisez une souris à 3 boutons sur un client Windows® connecté à une cible Linux®, le bouton gauche peut être mappé sur le bouton central de la souris à 3 boutons du client Windows.

Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel

Le système d'exploitation Windows 2000® ne prend pas en charge les dispositifs USB composites, comme D2CIM-VUSB de Raritan, de la même façon que les dispositifs USB non composites.

En conséquence, l'icône de la barre d'état Supprimer le périphérique en toute sécurité n'apparaît pas pour les lecteurs mappés par D2CIM-VUSB et un message d'avertissement peut s'afficher lors de la déconnexion du dispositif. Raritan n'a constaté aucun problème à la suite de ce message.

Comportement des CIM MCUTP

Le stockage du numéro de série ou du nom des CIM n'est pas assuré sur le câble MCUTP, les ports de ce type se comportent donc différemment des autres CIM, particulièrement :

- Le nom du CIM n'est pas stocké.
- Le nom du port est un libellé associé au port tant que le type de ce dernier ne change pas en raison de la connexion d'un type de CIM différent.
- Les paramètres de cible ne peuvent pas être appliqués aux ports de ce type.
- Le numéro de série apparaît sous la forme N/A sur les affichages indiquant le numéro de série du CIM ou dans les entrées de journal.

Annexe D Foire aux questions

Dans ce chapitre

Chapitre 12

LX - FAQ

Question	Réponse
Qu'est-ce que Dominion LX ?	Dominion LX est une famille de commutateurs KVM sur IP économiques disposant d'une alimentation unique, d'un réseau local unique et des supports virtuels. Destinés aux petites et moyennes entreprises gérant moins de 75 serveurs, ces commutateurs permettent la gestion IP au niveau du BIOS de 8 ou 16 serveurs au moyen d'un accès à distance pour un ou deux utilisateurs.
Pouvez-vous décrire le client LX type ?	Le client type, habituellement un administrateur informatique ou un développeur/testeur de logiciels, travaille pour une entreprise petite ou moyenne qui a besoin d'un accès KVM sur IP à distance toutes fonctions à un prix économique. Les clients LX souhaitent des fonctions qui améliorent la productivité, telles que les supports virtuels, la fonction Absolute Mouse Synchronization™ et des interfaces pour utilisateurs à distance et locaux communes.
Quelle est la particularité de Dominion LX ?	L'unité LX offre un commutateur KVM sur IP toutes fonctions et de haute qualité à un prix abordable. Contrairement à d'autres produits dans la même fourchette de prix, elle prend en charge des fonctions d'amélioration de la productivité telles que les supports virtuels, la fonction Absolute Mouse Synchronization et une interface utilisateur par navigateur commune.
Quels types d'équipement informatique l'unité LX peut-elle gérer ?	L'unité LX peut gérer un équipement géré par ordinateur et en série, notamment des serveurs et des équipements informatiques, des équipements de télécommunications et des dispositifs réseau.
Quels types de fonctions de gestion à distance sont pris en charge ?	Dominion LX permet une gestion à distance hors bande fiable. Ceci inclut une gestion KVM sur IP au niveau du BIOS, des supports virtuels à distance et un accès facultatif par modem. L'unité LX permet une gestion à distance partout et à tout moment, quel que soit l'état du dispositif cible. Vous pouvez entrer au niveau du BIOS, lancer des diagnostics de matériel, redémarrer un serveur bloqué, installer des logiciels depuis des DVD et même réimager un serveur, depuis un emplacement à distance.
Qu'est-ce qui différencie Dominion LX des produits concurrents ?	Les produits concurrents sont habituellement des commutateurs KVM sur IP d'entrée de gamme disposant de fonctions limitées et d'une interface utilisateur démodée. Ils n'utilisent pas de fonctions standard telles que les supports virtuels, Absolute Mouse Synchronization, la résolution vidéo à distance 1920 x 1080 et de sécurité.

Question	Réponse
Quelle est la proposition de valeur de LX ?	Un commutateur KVM sur IP de grande qualité, à un prix économique, destiné aux équipes informatiques et de développement des petites et moyennes entreprises. La proposition de valeur de LX est basée sur un accès à et sur la gestion à distance des serveurs et d'autres dispositifs informatiques, à tout moment et partout. Les clients LX bénéficient des avantages suivants : • frais de déplacement réduits ; • productivité accrue ; • délai moyen de réparation réduit ; • services de qualité supérieure.
Questions techniques	
Quels sont les modèles LX disponibles ?	La famille Dominion LX comprend trois modèles KVM sur IP. DLX-108 est un commutateur à 8 ports prenant en charge une session utilisateur à distance et un utilisateur local. DLX-116 est un commutateur à 16 ports prenant en charge une session utilisateur à distance et un utilisateur local. DLX-216 est un commutateur à 16 ports prenant en charge deux sessions utilisateur à distance et un utilisateur local.
Quelles sont les fonctions matérielles ?	Dominion LX dispose d'un boîtier de taille 1U comportant 8 ou 16 ports de serveur, d'une alimentation unique, d'un réseau unique d'un gigabit, d'un port local USB avec un accès par modem facultatif.
Qu'est-ce qui différencie Dominion LX de Dominion KX II ?	Dominion KX II est un commutateur KVM sur IP sécurisé et haut de gamme de Raritan conçu pour l'entreprise. Avec des modèles prenant en charge jusqu'à 64 serveurs et 8 utilisateurs à distance, KX II est destiné aux grandes et moyennes entreprises gérant des centaines ou même des milliers de serveurs. Dominion KX II est le commutateur le plus fiable et le plus sécurisé du marché et comporte une double alimentation, un réseau local double, un module de chiffrement FIPS 140-2 et une authentification par carte à puce/CAC. Dominion LX est une famille de commutateurs KVM sur IP économiques, destinés aux petites et moyennes entreprises gérant jusqu'à 75 serveurs. LX permet la gestion IP au niveau du BIOS de 8 ou 16 serveurs au moyen d'un accès à distance pour un ou deux utilisateurs.

Question	Réponse
Quelles sont les fonctions standard de Dominion LX?	Les fonctions standard de Dominion LX sont les suivantes : • Support virtuel • Synchronisation absolue de la souris • Interface utilisateur à distance/locale commune par navigateur • Résolution vidéo à distance 1920 x 1080 • Authentification locale et à distance (LDAP/AD/Radius) • Autorisations d'accès aux ports et administrateur • Double pile IPv6/IPv4 • Balayage des ports et vues en miniature • Fonction multiniveau (mise en cascade) avec d'autres commutateurs LX • Accès par modem • Fonctions de sécurité de base Reportez-vous au document **Dominion LX Features and Benefits** (Fonctions et avantages de Dominion LX) pour plus d'informations.
Quelles fonctions KX II ne sont pas disponibles dans LX ?	Les fonctions KX II suivantes ne sont pas disponibles dans LX : • Gestion centralisée CommandCenter® Secure Gateway (CC-SG) • Accès mobile via iPad® et iPhone® (CC-SG obligatoire) • Prise en charge des serveurs lames • Fonctions audionumériques sur IP • Module de chiffrement FIPS 140-2 • Prise en charge des cartes à puce/CAC • Bannière de connexion sécurisée • Gestion de l'alimentation à distance intégrée • Options de lancement d'écrans doubles et de clients KVM
Quels modules CIM (clés de serveur) l'unité LX peut-elle utiliser ?	Dominion LX peut utiliser : (1) les CIM Dominion standard et de support virtuel, (2) les CIM-câble MCUTP économiques et (3) les CIM série P2CIM-SER.
Qu'est-ce qu'un CIM-câble MCUTP et en quoi peut-il m'être utile ?	Pour les clients qui n'envisagent pas d'utiliser des supports virtuels et la synchronisation de souris absolue, les CIM-câbles MCUTP offrent une alternative économique aux CIM Dominion. Le CIM-câble est un CIM et un câble Cat5 intégrés disponibles dans différentes longueurs.
La gestion centralisée est-elle disponible pour Dominion LX ?	La gestion centralisée n'est pas une fonction standard de Dominion LX.

Question	Réponse
Que désigne le terme Support virtuel (virtual media) ?	Cette fonction puissante permet à un utilisateur d'effectuer le montage de lecteurs et de supports depuis son ordinateur sur des serveurs distants lors d'une connexion KVM. Cette méthode est idéale pour installer des logiciels, exécuter des diagnostics de matériel, transférer des fichiers et même réimager un serveur à distance.
Quels types de supports virtuels Dominion LX prend-il en charge ?	Dominion LX prend en charge les types de supports virtuels suivants : lecteurs CD/DVD internes et connectés USB, dispositifs de stockage de masse USB, lecteurs de disque dur PC et images ISO locales et distantes.
Que désigne Absolute Mouse Synchronization ?	Cette technologie élaborée par Raritan permet aux curseurs locaux et distants d'être synchrones dès le départ. Vous n'avez donc pas à modifier manuellement les paramètres de souris sur chaque serveur cible.

Index

Raritan.

Raritan.

P

R

S

Raritan.

Etats-Unis/Canada/Amérique latine

Lundi - Vendredi
8h00 - 20h00, heure de la côte Est des Etats-Unis
Tél. : 800-724-8090 ou 732-764-8886
Pour CommandCenter NOC : appuyez sur 6, puis sur 1.
Pour CommandCenter Secure Gateway : appuyez sur 6, puis sur 2.
Fax : 732-764-8887
E-mail pour CommandCenter NOC : tech-ccnoc@raritan.com
E-mail pour tous les autres produits : tech@raritan.com

Chine

Beijing

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-10-88091890

Shanghai

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-21-5425-2499

Guangzhou

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-20-8755-5561

Inde

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +91-124-410-7881

Japon

Lundi - Vendredi
9h30 - 17h30, heure locale
Tél. : +81-3-3523-5991
E-mail : support.japan@raritan.com

Europe

Europe

Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +31-10-2844040
E-mail : tech.europe@raritan.com

Royaume-Uni

Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +44-20-7614-77-00

France

Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +33-1-47-56-20-39

Allemagne

Lundi - Vendredi
8h30 - 17h30, CET (UTC/GMT+1)
Tél. : +49-20-17-47-98-0
E-mail : rg-support@raritan.com

Melbourne, Australie

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +61-3-9866-6887

Taiwan

Lundi - Vendredi
9h00 - 18h00, UTC/GMT - Heure normale 5 - Heure avancée 4
Tél. : +886-2-8919-1333
E-mail : support.apac@raritan.com